Secure Embedded Processing Solutions *for the* INTERNET *of* TOMORROW

Lutz van Remmen; Sales Manager Central&East Europe
SECURE, EMBEDDED PROCESSING SOLUTIONS for the

INTERNET of TOMORROW

The Internet of Tomorrow is the **advancement** of the Internet of Things (IoT) where **secure solutions** exist across every **touch point**, from end node to the network to the cloud.
... on the way and partly already here
Venture capitalists have invested 4.8M$ in a business that uses a wireless-connected collar to tell when cows are in heat.

... Everthing gets connected
IoT is Driving New Technology and Business Paradigms

- Sensing, Efficient, Networked, Secure, Everywhere. Tilting the direction of technology development and adoption, with significant implications for customers and also silicon vendors.

**Five verticals** get the most focus – While IoT will be found everywhere, 5 verticals are early in the adoption curve and offer a large market opportunity and the possibility for significant profits: Wearable Devices, Connected Cars, Connected Homes, Connected Cities, and the Industrial Internet.
Our Products Power the Internet of Tomorrow
…Solutions mapping from edge to Cloud

<table>
<thead>
<tr>
<th>Edge Node Solutions</th>
<th>IoT Gateway Solutions</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Xtrinsic Sensing</strong></td>
<td><strong>Cloud Solutions</strong></td>
</tr>
<tr>
<td><strong>Kinetis Microcontrollers</strong></td>
<td><strong>QorIQ Processors</strong></td>
</tr>
<tr>
<td><strong>Vybrid Controller Solutions</strong></td>
<td><strong>Built on Layerscape Architecture</strong></td>
</tr>
<tr>
<td><strong>i.MX Applications Processors</strong></td>
<td><strong>Accelerating the Network’s IQ.</strong></td>
</tr>
</tbody>
</table>

### Edge Node Solutions

- **Xtrinsic Sensing**
  - Intelligent Contextual Sensing.
  - The right combination of intelligent integration, logic and customizable software on the platform to deliver smarter, more differentiated applications.

- **Kinetis Microcontrollers**
  - Design Potential. Realized.
  - Industry's most scalable ultra-low-power, mixed-signal MCU solutions based on the ARM® Cortex™-M and Cortex™-M0+ architectures.

- **Vybrid Controller Solutions**
  - Rich Apps in Real Time.
  - Real-time, highly integrated solutions with best-in-class 2D graphics to enable your system to control, interface, connect, secure and scale.

- **i.MX Applications Processors**
  - Your Interface to the World.
  - Industry's most versatile solutions for multimedia and display applications, with multicore scalability and market-leading power, performance & integration.

- **QorIQ Processors**
  - Built on Layerscape Architecture
  - Industry's first software-aware, core-agnostic networking system architecture for the smarter, more capable networks of tomorrow – end to end.
In the News…Wearables has Crossed the Big Scary Chasm…
Automotive will be 2\textsuperscript{nd} largest $ generator on the IoT

- **Advise**
  - Tyre pressure
  - Brake wear
  - Service intervals
  - Insurance & toll services

- **Entertain**
  - Dig radio
  - Connected games
  - Streaming video
  - Internet/phone services

- **Assist**
  - Optimised routing
  - Blue wave
  - Optimum speed
  - E-brake lights
  - OTA software updates

- **Control**
  - Emergency braking
  - Adaptive cruise control
  - Road geometry tracking

---

**ITS**
- Big Data

**V2I CLOUD**
- DSRC
- Collision Avoidance
- Wifi, 3G, 4G, ...
Simplified Autonomous Vehicle Model

«Intelligent vehicles are a set of agents which integrate multi-sensor fusion-based environment perception, modeling, localization and map building, path planning, decision making and motion control.»
Prof. Cheng - 2011
Smart Factory - Industry 4.0

Smart Factory:
• Communication of M2M and machine-to-product all in interaction with people

• Connected objects trigger and deliver information and data for decisions.

• Processing and distribution of information in real time
Home Automation

Lighting  HVAC  Motor Control  Scenes  Entertainment  Appliance
Mobile Internet Control  Security  Surveillance  Sprinkler  Alarm
Timer  Energy Saving
IoT - The challenge for Semiconductors

More connectivity, more data means......

- increased Security requirements
- Adds SW complexity
- Requires More performance
- Requires more power

The implementation of security varies by area.
Freescale strategy to enable the IoT

We optimize the workloads produced by this Big Data explosion

We continue to shrink power envelopes, and optimize performance / power ratios

We continue to expand hardware-level security, and increase product lifecycles and reliability
I THINK MY NEST SMOKE ALARM IS GOING OFF. GOOGLE ADWORDS JUST PITCHED ME A FIRE EXTINGUISHER AND AN OFFER FOR TEMPORARY HOUSING.
End Node Security
Interconnected (IoT) Devices

90% of interconnected devices collected Personal Data

70% have serious vulnerabilities to attacks**

70% of devices were unencrypted**

FTC looking at IoT security legislation***

5X number of connected devices by 2020*

2015

2020

More unmanned (IoT End Nodes) than manned internet connections (PC, Smartphone)

90% of interconnected devices collected personal data.

70% of devices have serious vulnerabilities to attacks.

70% of devices were unencrypted.

FTC looking at IoT security legislation.

5X more connected devices by 2020 compared to 2015.

*Gartner excluding PC/Smartphones  **From a recent study by HP  ***FTC report Jan 27th
Researchers at the University of Texas have succeeded in hijacking a 213-foot yacht as it sailed from Monaco to Rhodes on the Mediterranean Sea, by overriding its GPS signals.

Internet of Things nodes are insecure

Early morning motorists got a shock yesterday when digital car park signs were tampered with by computer hackers and displaying an obscene message.

Tests revealed that the Hub was passing unencrypted data to the control device without authentication. Anybody on the network could detect the hub and run commands.

BLAST THE HORN, CONTINUING EVEN AFTER CAR TURNED OFF
PREVENT CAR FROM POWERING DOWN, DRAINING BATTERY
CHANGE SPEEDOMETER AND GAS GAUGE AT WILL
ABRUPTLY TIGHTEN DRIVER'S AND PASSENGER'S SEAT BELT

CAUSE ENGINE TO ACCELERATE (CAN BE OVERRIDDEN WITH THE BRAKE)
TURN HEADLIGHTS ON OR OFF WHEN LIGHTS LEFT ON AUTO
DISABLE POWER STEERING OR JERK THE WHEEL
SLAM ON BRAKES AT ANY SPEED

Researchers at the University of Texas have succeeded in hijacking a 213-foot yacht as it sailed from Monaco to Rhodes on the Mediterranean Sea, by overriding its GPS signals.
Industrie 4.0 – the internet has come to the factory and so have the attackers

“Security budget slide despite 48% increase in cyber attacks”

“PwC estimates that the average cost of managing and mitigating breaches rose to $2.7m per incident…”

“But the numbers of reported security incidents increased 48 per…”

Blackout
Ein Hacker brauchte nur zwei Tage, um die Kontrolle über die Stadtwerke in Ettlingen zu übernehmen. Er zeigte: Die Stromnetze in Deutschland sind nicht sicher.

von Christiane Gretz | 10. April 2014 - 08:00 Uhr

Botnetz scannt das Internet mit Hilfe von gehackten Endgeräten
Security: What to Achieve

Authentication
I can prove to another party that I am Lutz and only Lutz

Non-repudiation
I can send a message, but cannot later claim that I did not send it.

Validation
I can send a message, and can guarantee that it was not altered during transmission

Secrecy
I can send a message and know that, even if it is intercepted, it cannot be read

Protection
I want my equipment to prevent compromises in security
Security: How to Achieve

**Authentication**
I can prove to another party that I am User 12345 and only User 12345

**Non-repudiation**
I can send a message, but cannot later claim that I did not send it.

**Validation**
I can send a message & guarantee it was not altered in transmission.
I can run firmware and guarantee that it has not been altered.

**Secrecy**
I can send a message and know that, even if it is intercepted, it cannot be read.

**Protection**
My equipment must:
- Prevent compromises in security,
- Detect if system is tampered with,
- Store secret keys

- Asymmetric Ciphers ‘Public Key’
- Hashes & secure boot
- Symmetric Ciphers
- Hardware
Freescale Understands Security
Experience in developing security IP & providing certified security solutions for networking & industrial markets

**Proven Security Expertise**

- 40+ years of experience developing Information security solutions
- 150+ security patents
- 5000+ man years and $1.7 B invested to date
- Dedicated security technology Centers of Excellence
- Broad portfolio of cryptography and platform assurance IP.

**Cutting Edge Security IP & Product Portfolio**

- Cryptography (message encryption, decryption and authentication)
- Trust Architectures (secure boot, anti-cloning)
- Content Inspection (intrusion detection and prevention)
- Patented hardware engines for security, deep packet inspection, and pattern match
- Support for all known cipher suites, FIPS140-2 certifiable
- Efficient, scalable solutions in all processor families

**Robust Tools & Solid Ecosystem Partner Solutions**

- Extensive Tool Suite (hardware and software) available for customer evaluation
- VortiQa software toolsuite for control centre, monitoring control and home gateway applications
- Certified, Third-party software suite
- Driving Standards like Thread
Technology to secure the IoT

<table>
<thead>
<tr>
<th>Kinetis Microcontrollers</th>
<th>Automotive MCUs / MPUs</th>
<th>iMX Trust Architecture</th>
<th>QorIQ Layerscape Trust Architecture</th>
</tr>
</thead>
<tbody>
<tr>
<td>K-Reliance</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

- Secure Storage
- HW Firewalls
- HW Random Number Generation
- Secure Clock
- Trusted Execution
- HW Cryptographic Accelerators
- High Assurance Boot
- Secure Debug:
- Tamper Detection
Example: Microcontroller System Security

Kinetis MCUs Enable

- Node Authentication
- IP protection
- Secure Communication
- Tamper protection

- Hardware random number generator
- Protected Flash memory
- Memory protection unit
- LAN PAN WAN
- Integrated FLASH
- Peripherals
- CPU
- SRAM
- Unique chip identifier
- Secure key storage, Unique chip ID
- Encrypted communications
- Restrict external code accesses
- Tamper detection, Secure RTC

Hardware cryptographic acceleration
Summary and Conclusion:

Security is paramount for the safe and reliable operation of IoT. Security is the foundational enabler of IoT.

Deeply embedded endpoint devices need to be secured imposing additional challenges.

Security becomes a safety topic.

Security requirements drive technology requirements.

Security is a complex subject. Customers and suppliers and consultants have to work hand in hand.

Freescale understands what is needed to secure IoT from the end node to the cloud.
Freescale Enabled Devices
Industrial Automation

Arcturus uCP1020
Dual-core, QorIQ P1020 processor running at 800 MHz
Power to aggregate device communication from a remote site, using VPN-level secure connectivity.

IoT Gateway Reference Design
LS1021A-IoT gateway reference design based on the QorIQ LS1021A processor
Multi-service secured industrial IoT Gateway for building and factory automation and smart energy data concentrators.

Spiri Programmable Flying Robot
i.MX 6 applications processor
Airborne robot to survey terrain, detect land mines, water plants, report the news and even save a few lives along the way.
Freescale enabled Devices

Automotive

**Digital instrument cluster**

i.MX 6 applications processor running INTEGRITY RTOS

An ideal platform for automotive OEMs and Tier 1s looking to combine ISO 26262 safety certification with high performance, advanced 2D and 3D graphics.

**Demo: In Car Secure Network**

MPC5748G microcontroller, Hardware Security Module (HSM) embedded in MPC5748G MCU

Secure transfer of data to and from the vehicle is critical for safe and reliable operation.

**Demo: In Car Secure Network**

MPC5748G MCU, Hardware Security Module (HSM) embedded in MPC5748G MCU

The gateway module's central microcontroller needs to have robust on-chip security capabilities.
Freescale Enabled Devices

Wearables

Microsoft Band

Kinetis K24 Microcontrollers, Cortex M4 Low Power

First device powered by Microsoft Health, helps you achieve your wellness goals by tracking your heart rate, steps, calorie burn, and sleep quality.

SmartBackpack

Freescale FRDM-FXS-MULTI-B board attached to the FRDM-KL26Z and several additional Freescale sensors.

Monitor your devices without opening a zipper. The AMPL mobile app displays real-time battery levels and allows you to adjust charging priorities.

Orcam

i.MX6 Quad Application Processor

OrCam is an intuitive portable device with a smart camera designed to assist people who are visually impaired..

Confidential and Proprietary | 27
Freescale Enabled Devices
Home Automation

Smoke and Carbon Monoxide Detector:
Kinetis KL1x general purpose MCU
Motion control light nightlight with remote smoke and carbon monoxide detector.

2 way audio 720P IP security camera
i.MX28 applications processor
Remote video monitoring via a Wi-Fi enabled camera, cloud-based streaming video service, and a mobile app

Big AssFan - Haiku® with SenseME
Kinetis K series microcontrollers
Ceiling fan to think and make decisions to keep you comfortable automatically:
Secure Embedded Processing Solutions for

INTERNET of TOMORROW

freescale™