Security for Secure IoT: Advanced Architectures for IoT Gateways

Simon Forrest
Director of Segment Marketing, Consumer Electronics

www.imgtec.com

Imagination Technologies

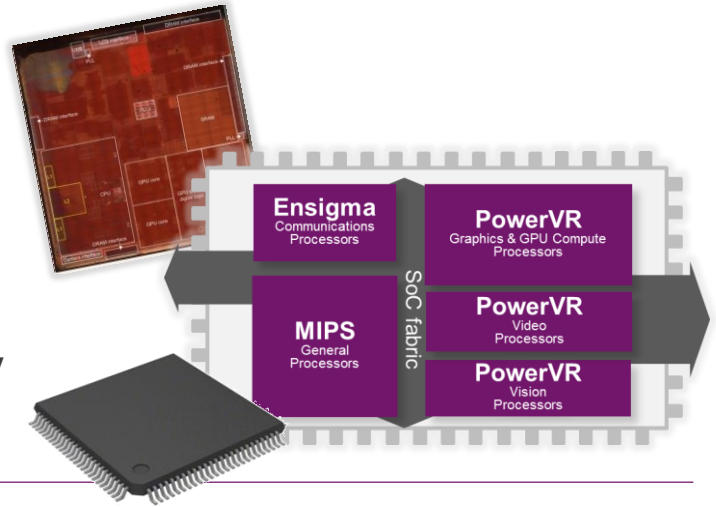
Company overview

A world leader in silicon and software IP

- 1,400 employees; over 80% in engineering
- UK headquarters with offices worldwide
- £120 revenue in FY2016

Products

- Embedded **graphics**, GPU compute and **video** IP
- CPU **processor** IP – MIPS architecture
- **Radio communications** IP – DAB, Wi-Fi and Bluetooth



Customer success

- Imagination supplies technology to silicon chip vendors
- Over **10 billion** products using Imagination's technology
- Shipments of over **3 million per day**

Agenda

Security for Secure IoT: Advanced Architectures for IoT Gateways

- **Challenges presented by IoT in the home**
- **Current solutions**
- **Virtualization**
  - What is it? How can it be used?
- **A new architectural approach**
  - Using virtualization
- **Benefits**
- **Summary and conclusions**

The challenge of IoT in the Smart Home

Multiple standards, multiple networks, multiple domains

- **Home Networking**
  - 802.11ac → 802.11ax
    - Most sensitive network; highly secure
- **IoT & Smart Home**
  - 802.15.4 *(ZigBee, 6LowPan, Thread)*, Bluetooth Smart, Z-Wave…
    - Sensors and actuators; home security; smart lighting; fitness and healthcare…
  - NFC
    - Device configuration
    - Transfer of network security credentials

Today's solution

Technically feasible but unsustainable

- **Throw hardware at it… IoT gateways**
  - Simple… but increases the "attack surface"
  - Weakness in one device → "pivoting" to others
- **Creates overlapping networks**
  - Gateways using the same networking protocols
  - Misuse of available spectrum → radio congestion → unreliable networks
- **Ultimately this topology is unsustainable**
  - One gateway per service. Why not aggregate?
  - Must improve security of the overall system
- **We need a new gateway architecture**

Hardware versus Software

Why adding IoT gateways has been the simple answer

Adding hardware is easy

- Vertical; targeted; solution-focused
- Self-contained; flexible
- Dedicated processing resources
- Additional radios, network interfaces, etc.
- Security through isolation

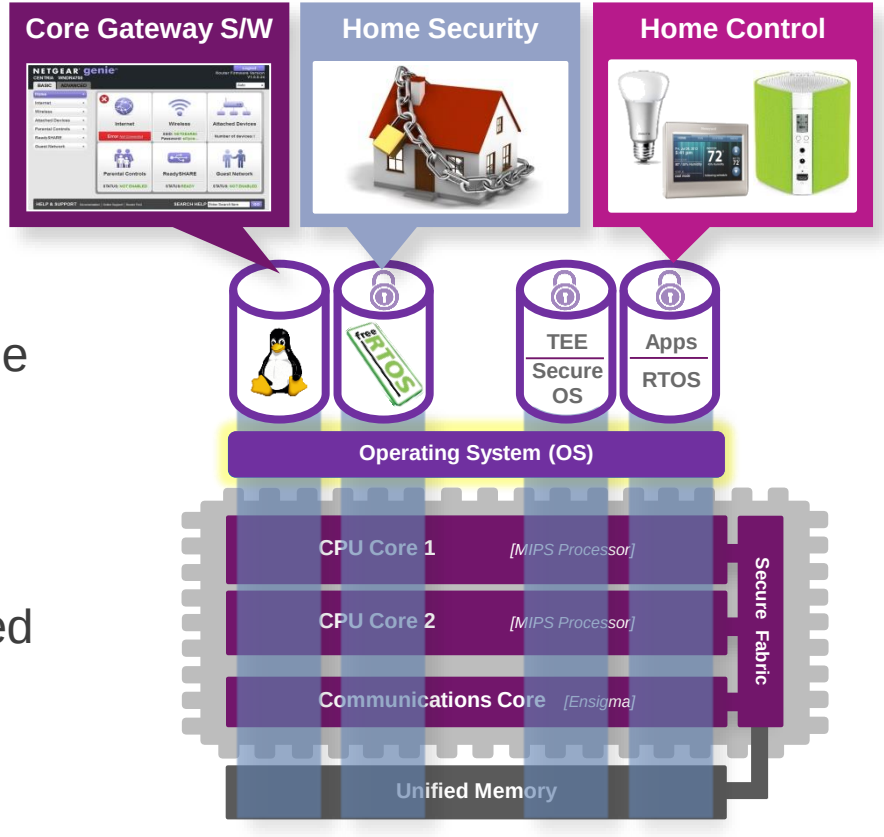
Adding software and services is hard

- Software integration challenges
- Diverse ecosystems
- Multiple standards
- Disparate operating systems, kernels, drivers
- Security: services must trust each other
- Impact upon time-to-market
- Quality assurance and testing

Virtualization

A brief introduction

- **Key features**
  - Hypervisor manages access to all cores/resources on the SoC, peripherals and external memory access
  - Allows creation of “containers” for multiple software environments
  - Several OSes run concurrently
    - Secure and isolated
  - Create and destroy containers as required
    - Static or dynamic
    - System reallocates resources



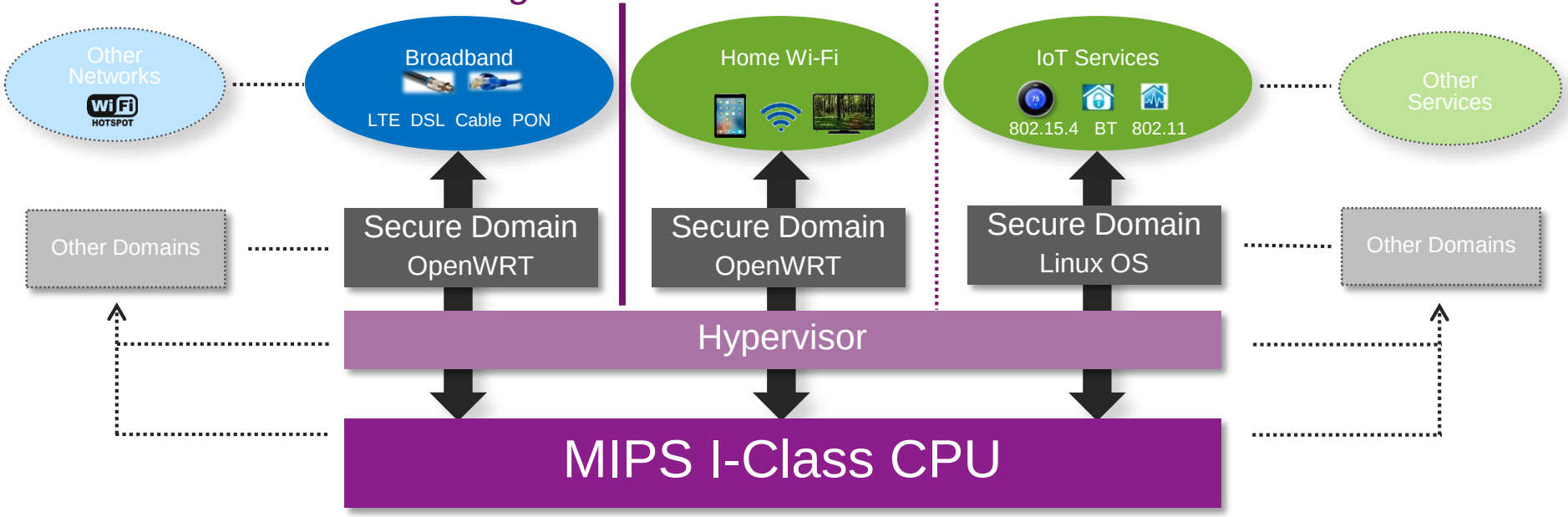
Other considerations

Challenge is to provide a secure environment in which applications can coexist

- Easy to install applications
- Protect essential core system services
- Safeguard other services
- Segregate data from applications that are not entitled to have access (e.g. network routing, healthcare data, lighting control, etc.)
- Flexible to enable all use cases
- Easy for the consumer to understand and use

A new approach

Advanced architecture using hardware virtualization



- Single gateway supports disparate services
- Services are isolated from core software
- Maintains service continuity during upgrade
- Delivers security across all domains

Engineering benefits

New architecture → Improved security → Faster development

- **Core functions run concurrently alongside IoT services**
  - Existing OS and services continue to run, just as before
  - Isolate critical software and applications with guaranteed security
  - No software integration required to add or remove services
- **Multiple secure domains for IoT services**
  - Absolutely no impact to software running in other containers
  - Deploy appropriate OS for the task
- **Accelerated time-to-market**
  - Reduction in software development, QA, testing and certification

Operator benefits of virtualized gateways

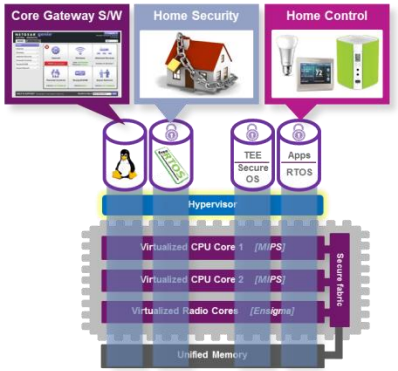
Driving business opportunity

- **Flexible deployment of IoT services**
  - Wider selection of service vendors
  - Maintain service continuity during upgrades
- **Low risk**
- **Reduction in hardware**
  - Environmental considerations
  - Simple solution for customers
- **Customer retention**
  - Increased consumer choice
  - Managing services throughout the contract
- **Security as standard**

Summary

Security for Secure IoT: Advanced Architectures for IoT Gateways

- **Security is essential in IoT**
  - Isolate devices, networks, data and services
- **Architecture for IoT gateways must evolve**
  - Tighter hardware integration → Eliminate gateway “clutter”
  - Reduce radio congestion → More reliable networking
  - Utilize existing resources and extend the gateway
- **Hardware virtualization provides the solution**
  - Faster time-to-market, more reliable products
  - Security “as standard”
  - Not only applicable to IoT hubs and gateways; sensors too!



www.imgtec.com