UNISOC Secure AIoT Solution

2019年中国上海嵌入式系统安全论坛

UNISOC Vision

UNISOC

UNISOC Today

4500+
90% R&D Engineers

14
Global R&D Centers

TOP3
Mobile Chipset Vendor Globally

600M
Mobile Chipset Shipment Yearly

1300+
Customers Globally

TOP2
Wi-Fi Shipment in China

No.1
LNB/Satellite Tuner Market Share

95%
Global Market Coverage

UNISOC Secure AIoT Solution

The Cloud
Data Processing and Mining
Machine Learning, Training and Management

The Edge – Smart Gateway
Data Analytic, AI Inference and Security
Powered by UNISOC MEC Platform

The Thing – Smart Device
Data Collection and Controller
Powered by UNISOC AI PSA Platform

Flexibility and scalability of vendor protocol awareness and trusted operation

Communicate between different management protocols and networks

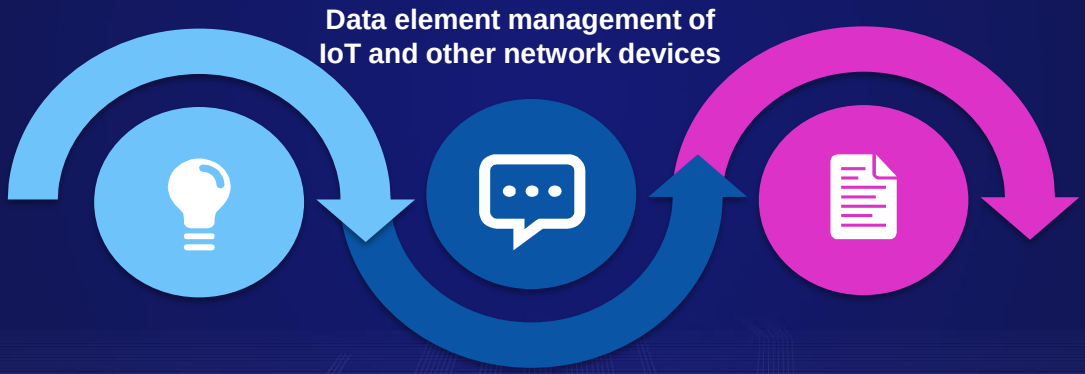
Trusted operation and security management

Interoperability of different technologies
e.g. Wi-Fi, Bluetooth, Zigbee

Device on-boarding and deployment

UNISOC

24/7 real time management and failure prediction



Smart planning and interference management

Spectrum and bandwidth planning and real time interference management improve network efficiency

e.g. Better multi-band operation

RF heat map and performance statistics can be monitored more effectively

e.g. Home Design heat map can be optimized for real situation – interference, decoration, etc.

IoT device security concern

Device lost, end of life cycle

Data stored in external storage could be exposed

Malware applications and libraries

Malware applications might introduce risks to online shopping credentials, copy-right license, network key, application keys

Network attack

Wi-Fi, TCP/IP and higher layer protocols like HTTP, FTP and SSH are facing attacks all the time, attackers could control the devices

Physical tamper

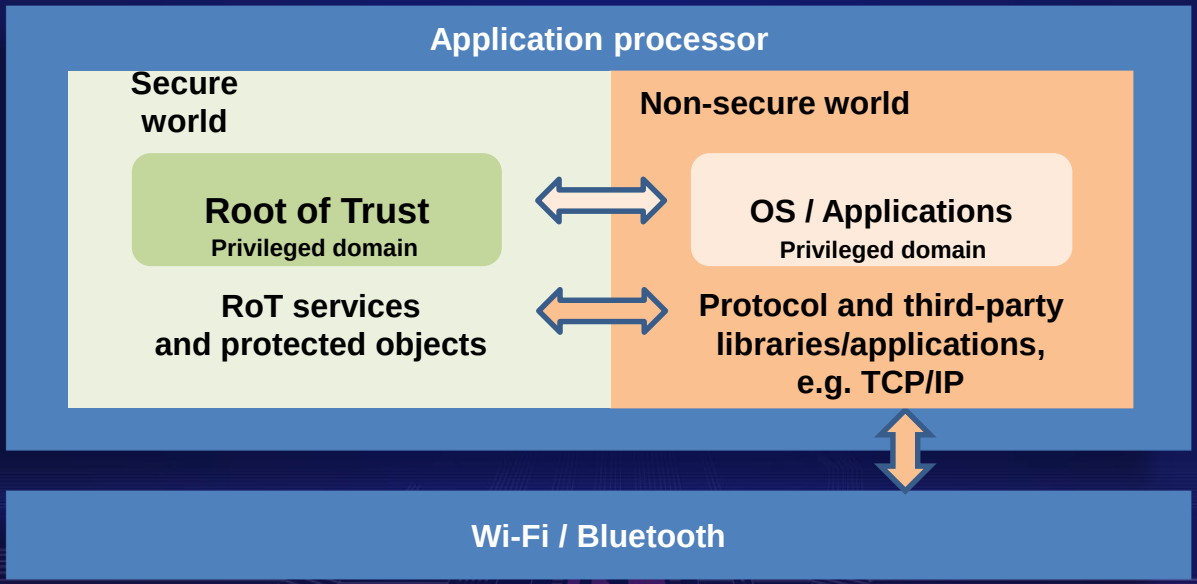
Attacker could get everything once breaking into the system

UNISOC

UNISOC PSA Platform

Dual Core ARM CM33
Trusted operation partition and secure peripherals
Secure boot and storage, key protection and attestation
Secure clock and debug, rich feature cipher engine
Advanced low power consumption architecture
Wi-Fi 5 2x2 2.4/5 GHz dual band, MU-MIMO, location
Bluetooth audio, long range, mesh and direction finding
RF and PA/LNA/Switch integrated
Advanced multiple radio coexistence feature

UNISOC PSA Platform



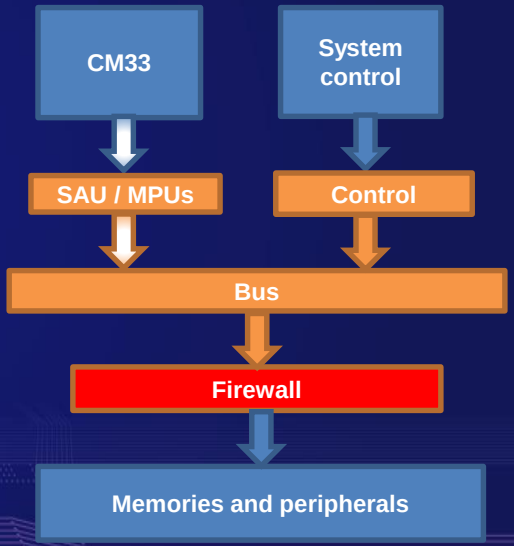
Application processor isolation

Processor working model
- Secure / non-secure and privileged / un-privileged

Working mode switching
- Developer controllable for specific purpose

Secure world partition
- Security Attribution Unit
- Memories and peripherals firewall

Privileged domain partition
- Memory Protection Unit



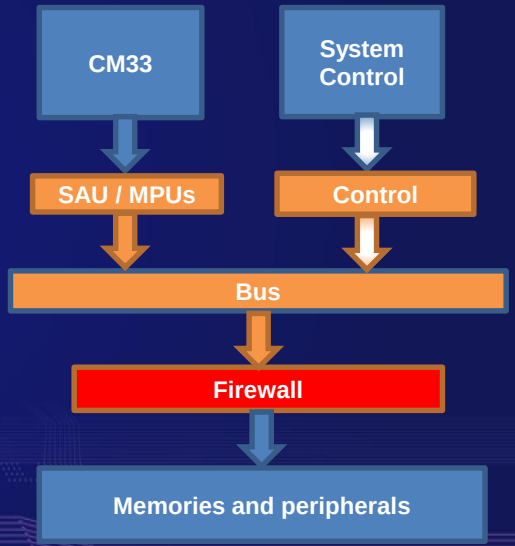
System control plane isolation

Control plane working modes
- Secure / non-secure

Working mode switching
- Programmable security attribute of bus request

Secure world partition
- Memories and peripherals firewall

Privileged domain partition
- Bus initiator identification and filtering

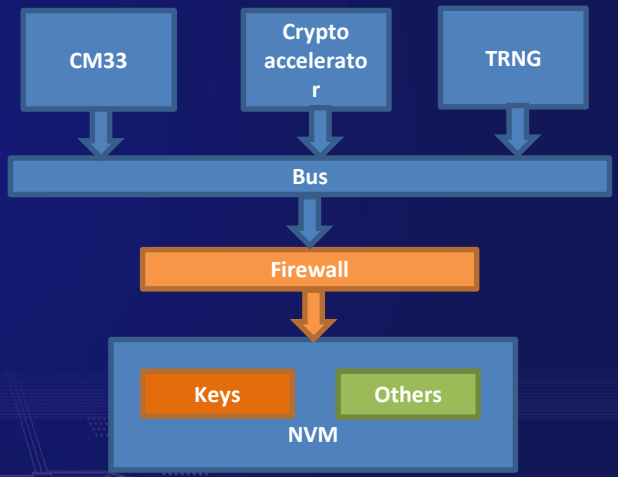


Secure communication and storage

High speed crypto acceleration
- AES, RSA, ECC, Hash, HMAC etc.

Hardware based confidentiality and protection
- Hardware unique key
- Master keys
- Key isolation and concealment

Security level improvement
- True Random Number Generator

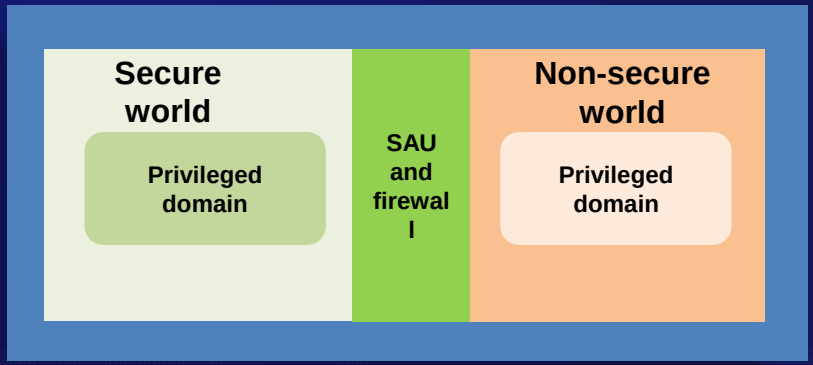


System building and maintenance

Secure boot
- System integrity check
- RSA-PSS and ECDSA
- Anti version rollback

Attestation
- Health status report
- Device Self Identification

Secure OTA upgrade



Product life cycle management

Manufactured

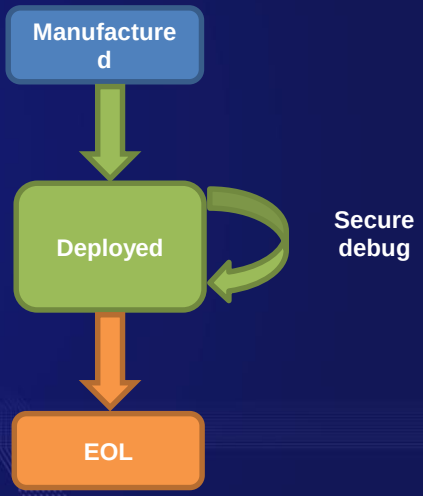
Trusted clock and RF calibration

Deployed

Root certificate installed
Keys installed
Image installed
Secure-debug enabled or debug disabled

End of life

Disable keys so that all the data encrypted with these keys will not be usable any longer



UNISOC

Q and A


THANKS