Platform Firmware Resiliency in Automotive Applications

Presenter: Peter Kwak, Principal Embedded Solutions Engineer, Korea

Date: January 25, 2022

MICROCHIP

Automotive Growth Drivers

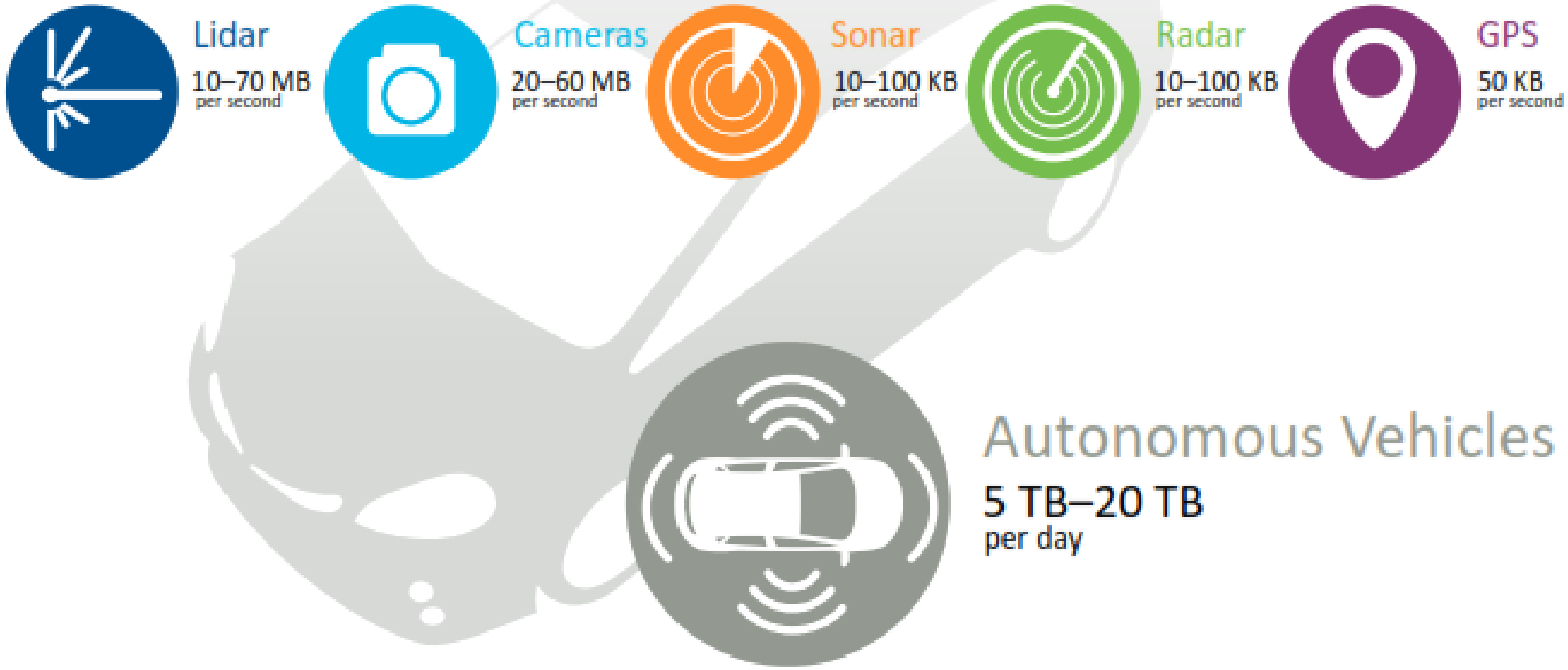
Infotainment systems and extension of the ”consumer world” into automotive

Assisted and autonomous driving – while maintaining vehicle and road safety

Electrification of vehicles and related infrastructure

Automotive cybersecurity

Data Center on Wheels

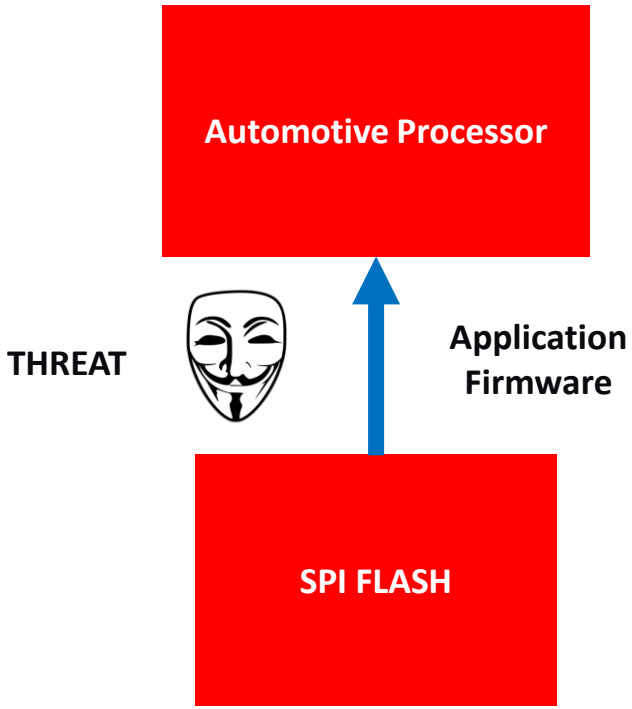


Firmware Vulnerabilities in Automotive

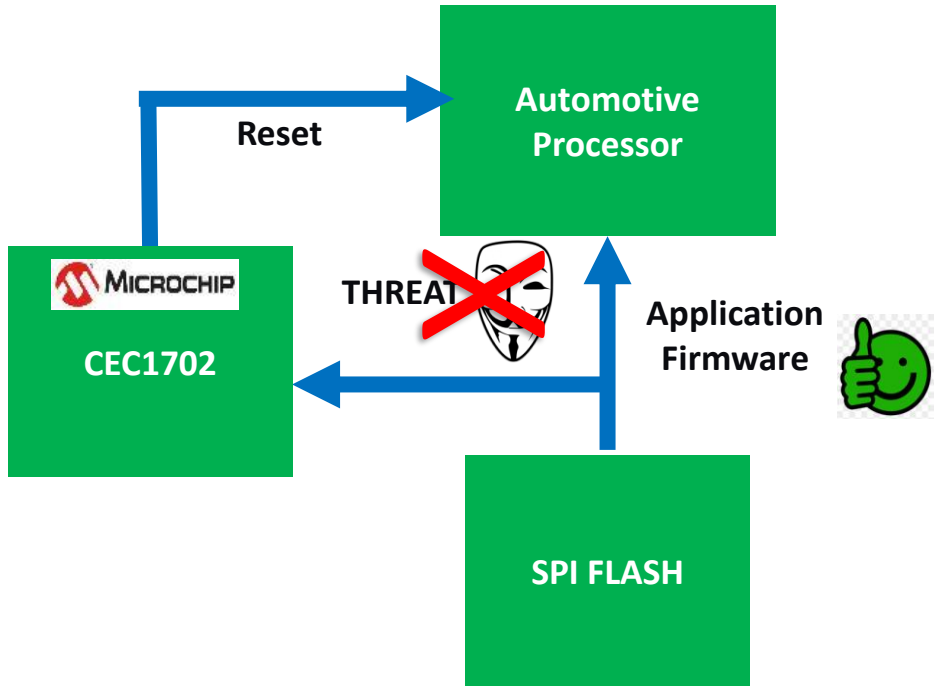
- One of highest-value system attacks
- Historically little to no protection
- Launching point for additional security breaches
- Keeping pace with security advances is challenging

Firmware Vulnerability and Protection Simplified

Unprotected Boot of Automotive Processor



Secure Boot of Automotive Processor



Automotive Platform Firmware Protection

CEC1702 Secure Boot Controller

Immutable HW Root of Trust

Hardware-based Code Authentication

Secure Firmware Updates

NIST 800-193 Platform Firmware Resiliency

Advanced Algorithms to Keep Pace with Change

AEC-Q100 Automotive Qualified

MICROCHIP

CEC1xxx Hardware Crypto Suite

Crypto Parametrics		CEC1302	CEC1702	CEC1712
Symmetric Encryption		AES128, AES192 and AES256		
		Modes: ECB, CBC, OFB, CFB, CTR		
Hashing		SHA-1, SHA-256	SHA-1, SHA-256, SHA-384, SHA-512	
Public Key Engine (PKE)	RSA	RSA-512 to RSA-2048	RSA-1024 to RSA-4096	
	ECC	Keys from 160 to 256 bits in GF(p)	192 to 521 bits in GF(p) 160 to 571 bits in GF(2m) Curve25519	
	DSA	No	ECDSA, EC-KCDSA, Ed25519	
	Other	No	Miller-Rabin Primality Testing	
		Modular Arithmetic Primitives		
Random Number Generator		True RNG		
		1K FIFO for pre-calculation		
Monotonic Counter		No	Yes	
User Programmable OTP		500 bits	2.5K bits	4k bits
Field Programmable		No		Yes
Memory Protection Unit		No	Yes	Yes
Secure Boot	Integrity	SHA256	SHA256	SHA-384
	Authentication	No	ECDSA-P256	ECDSA-P384
	Encryption (optional)	No	ECDH-P256 / AES-256	ECDH-P384 / AES-256
Attestation	DICE	No	1st Mutable Code	In ROM
	UDI	No	Factory Provisioned (optional)	
Temperature Range		0°C to +70°C	-40°C to +125°C	-40°C to +85°C
AEC-Q100 Qualification		No	Yes	No

- **CEC1702 updates:**
  - AEC-Q100 qualified
  - Recommended for automotive designs
- **CEC1712 new features:**
  - Key Revocation
  - Code Rollback
  - CNSA secure boot (P384)
  - FIPS 800-193 100% Redundant Boot
    - 2 independent SPI Flash
  - In-circuit programmable OTP

Securing Firmware Updates

MICROCHIP

CEC1702 Provisioning

Microchip Programming Services

- All provisioning communication uses PGP in a secure environment
- First article samples provided for customer approval

Information Provisioned in OTP:

- Keys for secure boot and for code encryption
  - Authentication public key for secure boot
  - ECDH1 private key for optional encryption; this key is encrypted
  - ECDH2 public key for optional encryption
- Customer OTP region
  - UDI, serial number, or other customer information

3rd Party Provisioning

- Application note available under NDA

Why Microchip?

- 20+ year proven security track record
- Minimizes impacts to legacy application processor code
- Scalable solutions from component to platform
- NIST 800-193 platform firmware resiliency
- Reference designs/development boards
- Factory and 3rd party secure provisioning
- SHIELDS UP! training for clients
- AEC-Q100 grade 1 qualification
- Design review services
- Client driven obsolescence
- Extensive GLOBAL design support to OEM/ODM and their customers

For More Information

- **Download the CEC1702Q-B2-E/SXVAO Datasheet**

- https://ww1.microchip.com/downloads/en/DeviceDoc/CEC1702-Autmotive-Data-Sheet-DS00003568A.pdf

Thank You