Flash Memory Summit

New Cybersecurity Regulations Require Innovative Memory Solutions

Adrian Cosoroaba

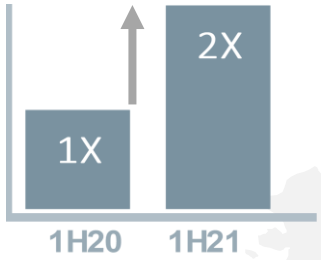
Winbond

35 YEARS OF NAND FLASH MEMORY INNOVATION

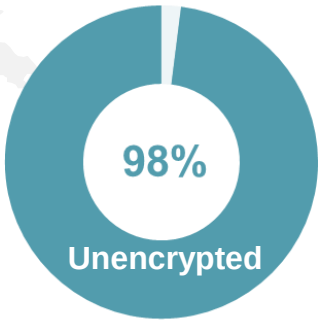
Agenda

- Security of IoT and Connected Devices
- Cybersecurity Regulation Trends
- Secure Storage Requirements
- Secure Flash Solution

Increasing Security Concerns in IoT Devices

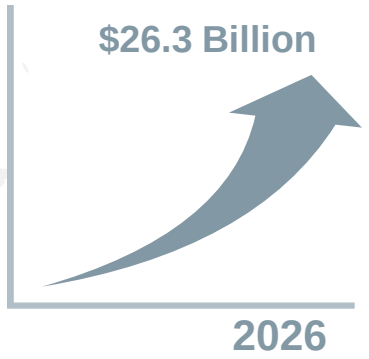


- The first half of 2021 saw **1.5 billion attacks on IoT devices** (more than double the total recorded in the first half of 2020), reported by Kaspersky.



- About **98%** of internet of things traffic data is **unencrypted** in 2020, reported by Palo Alto Networks.

- The average cost of a data breach in 2020 is **$3.86 million**, reported by IBM.

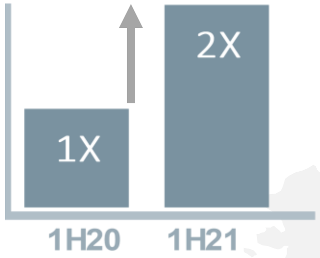


- The global endpoint security market to reach **$26.3 Billion by 2026**

* Kaspersky's research department, Sep 2021.
** 2020 Unit 42 IoT Threat Report by Palo Alto Networks, Mar 2020.
*** Cost of a data breach report 2021 by IBM.

Increasing Security Concerns in IoT Devices

Flash Memory Summit

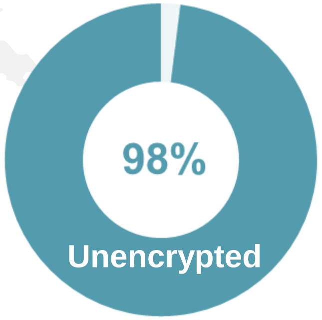


- The first half of 2021 saw **1.5 billion ttacks on IoT devices** (more than double th total record n the first half of 2020), rep d by Kaspers

96% are deployed without any security expertise.

Only 4% of deployed IoT products have security.

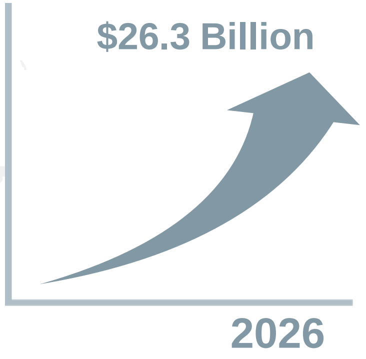
- A ... o Networks.



Cost
$

- Th ... is **$3.86 mil**

- The gl endpoi ecurity market to reach **$26.3 B ion by 2026**



* Kaspersky's research department, Sep 2021.
** 2020 Unit 42 IoT Threat Report by Palo Alto Networks, Mar 2020.
*** Cost of a data breach report 2021 by IBM.

35 YEARS OF NAND FLASH MEMORY INNOVATION

Agenda

Flash Memory Summit

- Security of IoT and Connected Devices
- Cybersecurity Regulation Trends
- Secure Storage Requirements
- Secure Flash Solution

35 YEARS OF NAND FLASH MEMORY INNOVATION

Security Regulations

Governmental Security regulations have major impact on systems integrators to implement HW security functionality

There are several other security standards and regulations in pipeline to become effective till 2024, including MFP, Automotive and Consumer IoT devices in the US, EU, Japan

EU Cybersecurity Regulations – RED

Flash Memory Summit

- The European Commission's (EC) Radio Equipment Directive 2014/53/EU (RED) establishes a regulatory framework for radio equipment. On Jan. 12, 2022, delegated regulation 2022/30/EU is published, enforcing compliance requirements to RED Article 3.3 (d, e and f).
  - The regulation **increases cybersecurity, personal data privacy and fraud protection** for applicable wireless devices available on the EU market: Mobile phones, tablets, laptops, networking devices, wireless toys, baby monitors, wearable devices, etc – **any wireless connected device is under the directive**
  - It takes **effect Feb. 1, 2022**, and **becomes mandatory Aug. 1, 2024**, giving device manufacturers a 30-month transition period.
  - New devices placed on the market, should comply with the new "cybersecurity" essential requirements, staring **Aug. 1, 2023**

- Complemented by a Cyber Resilience Act

35 YEARS OF NAND FLASH MEMORY INNOVATION

ISO/SAE 21434 Road Vehicle Cybersecurity

- ISO/SAE 21434 is International standard to establish a security lifecycle in the automotive environment
- The purpose is to ensure that OEMs and all participants in the Automotive supply chain have structured processes in place that support a "**Security by Design**" process. The standard applies to road vehicles including **ALL their components**, connections and software. **The importance of secure hardware development should not be underestimated**!

- In the **European Union**, the ISO/SAE 21434 will be mandatory for all **new vehicle types from July 2022** and will become mandatory for all **produced cars from July 2024**

Agenda

- Security of IoT and Connected Devices
- Cybersecurity Regulation Trends
- Secure Storage Requirements
- Secure Flash Solution

Why do we need Secure Storage?

VULNERABILITY

- Eavesdropping
- Unauthorized data read
- Unauthorized data/code manipulation
- Attacking memory interface

NO SECURITY MECHANISMS

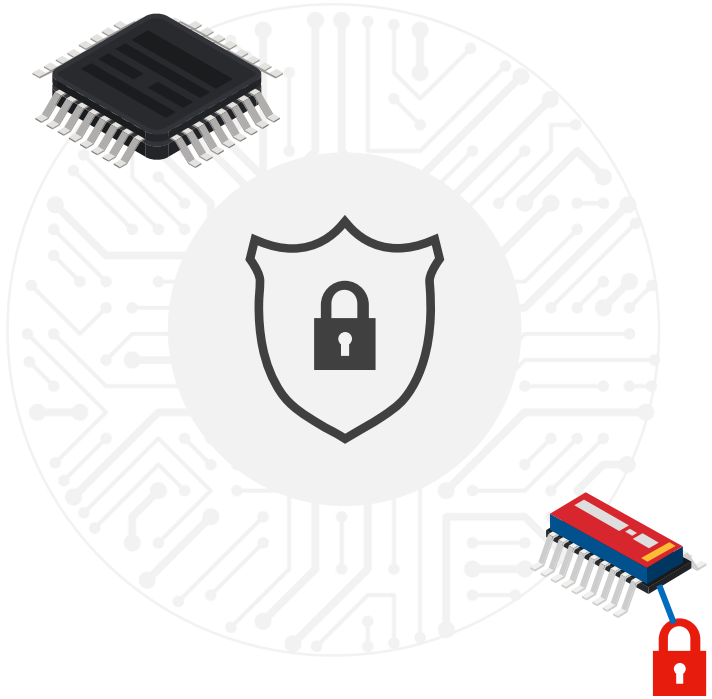
Standard memory devices have no security mechanisms. For most use cases, security must be extended from MCU to include the storage device (not rely only on MCU)

What is “a Secure Storage”?

Flash Memory Summit

The system needs
A secure storage device

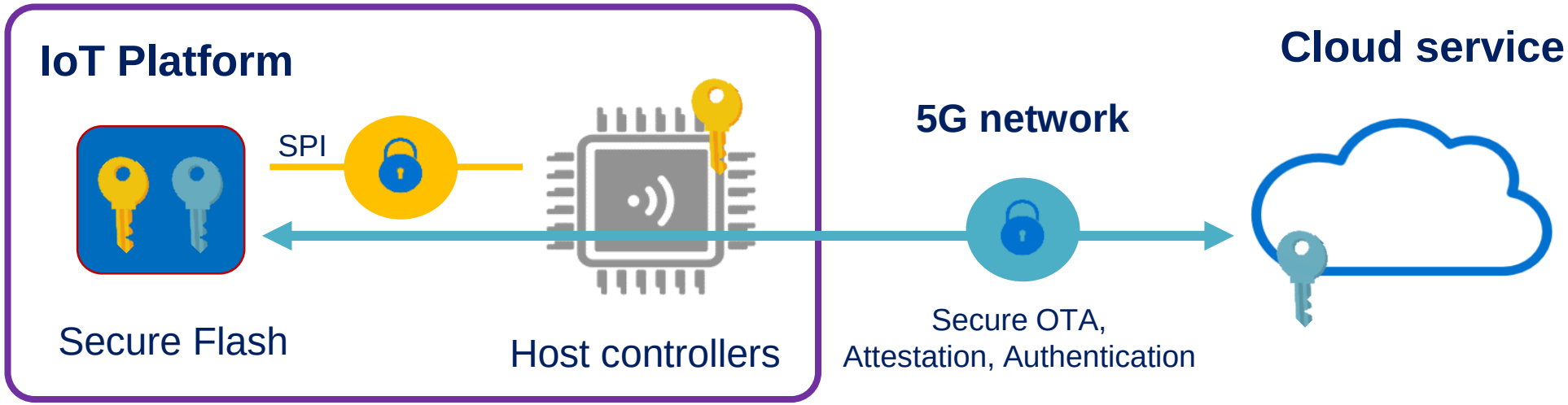
- The storage needs to be as reliable as an embedded storage
- The data stored inside the secure storage should be accessible only to authorized entities
- The stored data can only be modified by authorized entities
- System should keep track of changes made to the stored data and alert if outdated data is found



These storage devices must meet certification requirements
(SESIP, Common Criteria)

35 YEARS OF NAND FLASH MEMORY INNOVATION

Secure Storage for Connected Devices



Flash device becomes Active security component to complement MCU for platform assets protection : code, user data, credentials, keys

- Root of Trust
- Secure Data Storage
- Secure OTA Firmware Update
- Secure channel to cloud
- Platform Resiliency

GlobalPlatform SESIP Protection Profile For Secure External Memories

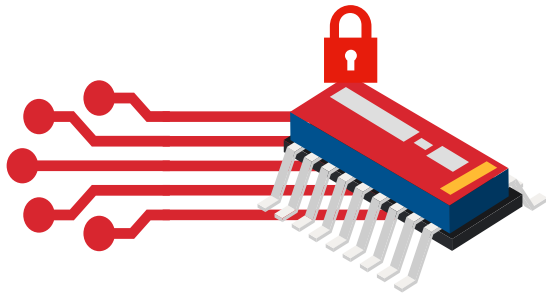
Flash Memory Summit

GlobalPlatform published SESIP profile for Secure External Memories (GPT_SPE_148)

- Evaluate a memory device as a “stand alone” component without relying on the security capabilities of the SoC/MCU

Required main security features

- Data is protected for integrity and authenticity
- Communication with the secure memory is protected
- Freshness of the memory content is guaranteed
- Physical attacker resistance

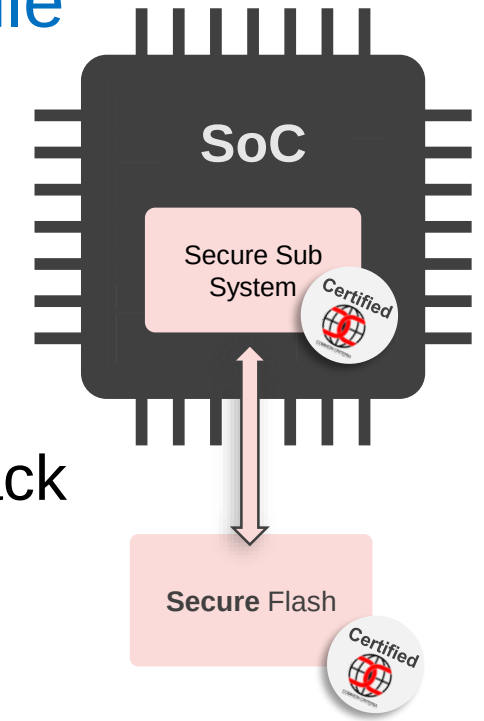


35 YEARS OF NAND FLASH MEMORY INNOVATION

Common Criteria Secure Sub-System PP0117

Flash Memory Summit

Eurosmart published Secure Sub System Protection Profile (PP0117) to address integration of security into SoC devices, leveraging external Secure Memory



Protecting data stored in external memory

- Protection from content abuse, replacement, replay and rollback
- Memory Interface protection from abuse
- Certified Secured Memory

35 YEARS OF NAND FLASH MEMORY INNOVATION

Agenda

Flash Memory Summit

- Security of IoT and Connected Devices
- Cybersecurity Regulation Trends
- Secure Storage Requirements
- Secure Flash Solution

35 YEARS OF NAND FLASH MEMORY INNOVATION

Secure Flash from Winbond

- **W77Q Serial SPI NOR Flash based on the standard SPI Flash**
  - **100% Drop-in replacement** for SPI NOR Flash
  - No need to redesign board or MCU
- **Advanced security features:**
  - **Root of trust** and Secure Boot
  - **Secure Over-The-Air firmware** update (Rollback protected)
  - **Firmware Resiliency**: Protection, Detection and Recovery
  - **Secure data storage**
  - Design is based on pure digital logic, no integrated MCU
- **Certified secure memory = Trusted and Proven Solution**
  - Common Criteria EAL2 and EAL5+, FIPS 140-3 CAVP, SESIP Certified
  - ISO21434 Automotive Cyber Security (in progress)

https://www.winbond.com/hq/product/trustme/

Thank You

Adrian Cosoroaba
cosoroaba@winbond.com

Please visit Winbond at Booth #719

