CyberSEC 2024

How Hardware Security Can Help AIoT Defend against Attacks in the Chain of Trust

Speaker: Connie Chen

PUFsecurity
AN eMemory COMPANY

Who we are .

PUFsecurity

Delivering integrated PUF-based **Security Subsystem IPs** that offer comprehensive protection unparalleled in the market

Drop-In IP-Blocks
(TRNG, Anti-Tamper, Crypto Engine)

ememory

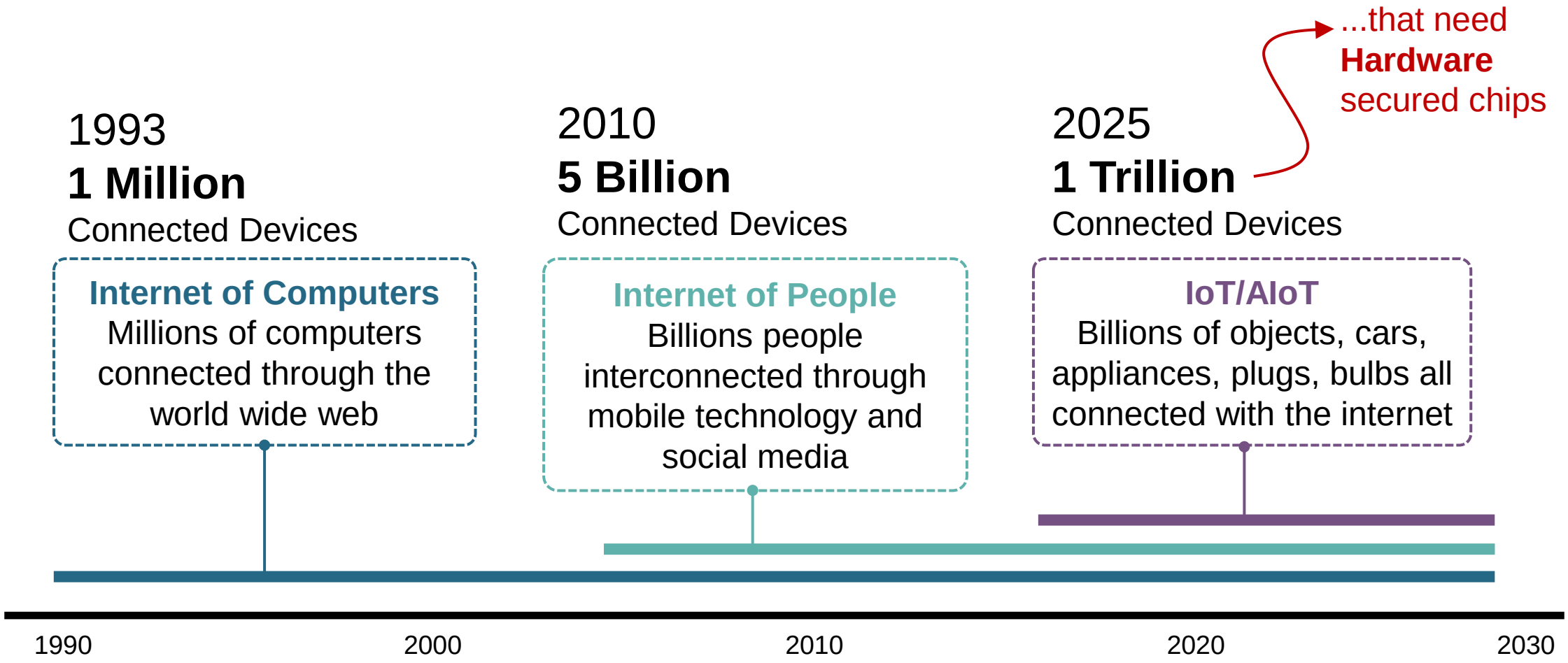
World's Largest Pure-Play **Non-Volatile Memory IP** provider with 550+ Process Platforms from 0.35μm down to 3nm

Hard Marco IP
(Anti-Fuse OTP, PUF)

Agenda

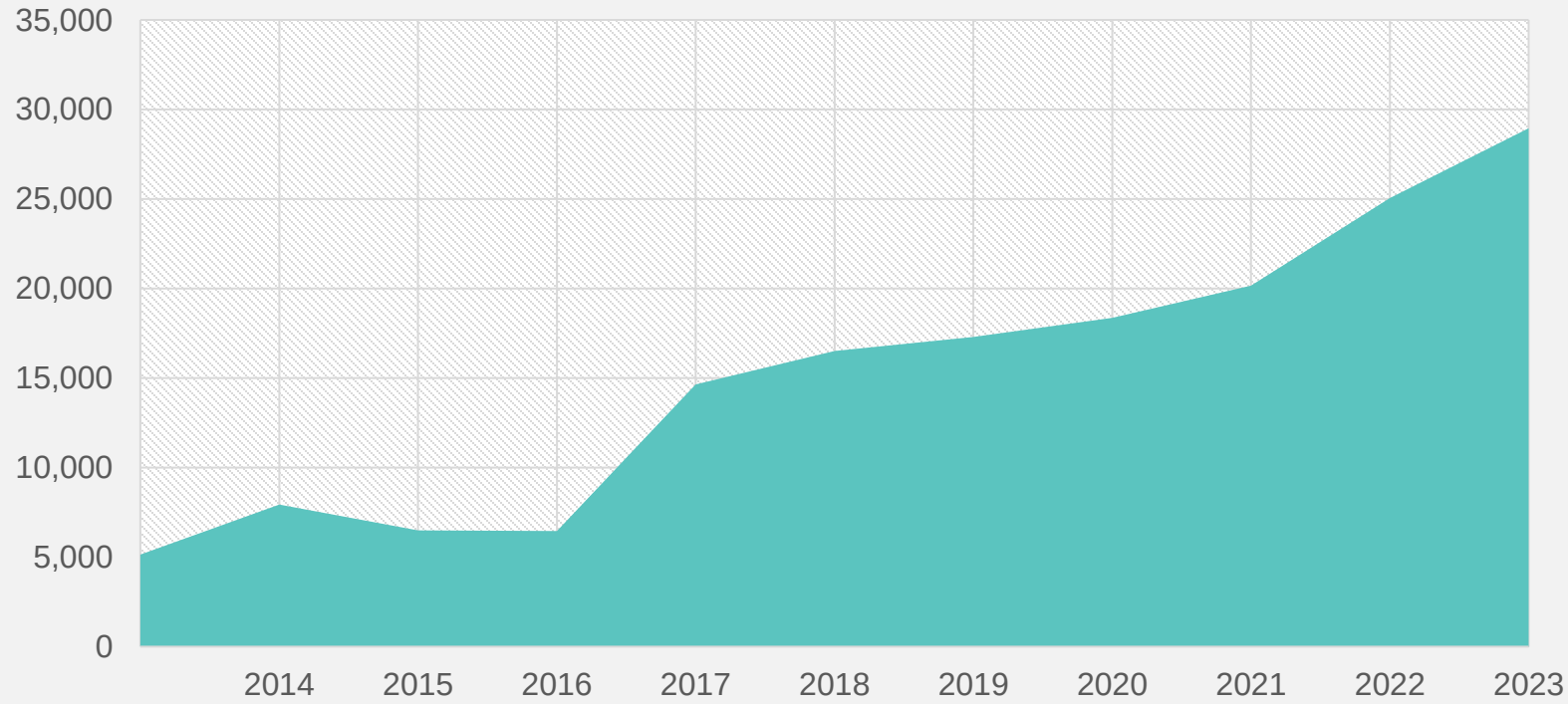
1. **Cybersecurity Threats & Trends**
2. Importance of Hardware Security
3. Chip Fingerprint
4. PUFsecurity Solution

The security challenges in **Connected Devices**



Increasing **Security Flaws**

Issued CVE Numbers
Count per Year

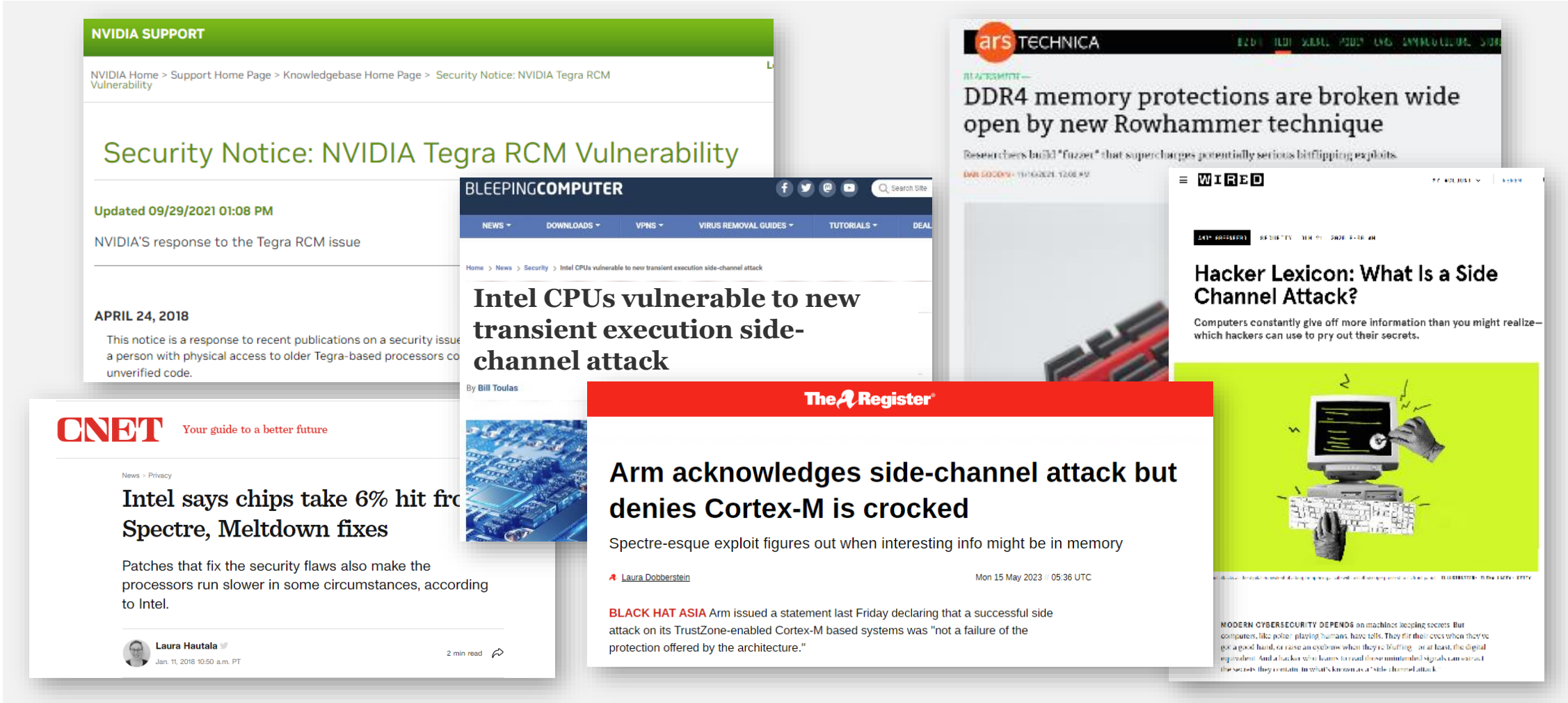


CVE

Stands for Common Vulnerabilities and Exposures. It is an industry list of publicly disclosed computer security flaws

Reference: CVE Org link, Hacker News link

Increasing Hardware Attack



Reference: NVidia link, CNET link, Beeping Computer link, The Register link, ARS link, Wired link

Agenda

1. Cybersecurity Threats & Trends
2. **Importance of Hardware Security**
3. Chip Fingerprint
4. PUFsecurity Solution

The Enigma Machine – **Data Encryption**

Confidential Data

Message

Bereiten Sie sich auf den Vormarsch des Westens vor. Nachschub und Verstärkung werden in zwei Tagen zu Ihnen stoßen

Cryptography Engine

Encrypted Cypher

```
1330 = 2tle = 1tl = 250 = QHM LVA =
CXOOL IMTWV BGJWA SZAEV KSEOY ZGPJY
YYVGZ KFUHJ DCRQO ZEJAR YVYXV CATUH
QEWBE TXBAC KZNFE RCVXX QKPLC POFVJ
BPXNH BNEPO EZHTC PFEJM VEUHZ HEBYC
XOETQ YKWJP RQXIV QFVMS DKCKQ OAUPZ
HTNFW IWUEP EYQDE KBGNR WPZJF HGVJX
NYXKM JHBGI GWBIV PCNWW BCBSG YWSGV
```

The Secret Key: The biggest threat was the enemy gaining access to the Codebook

Geheime Kommandosache / Nicht ins Flugzeug mitnehmen

Armee-Stabs-Maschinenschlüssel Nr. 28

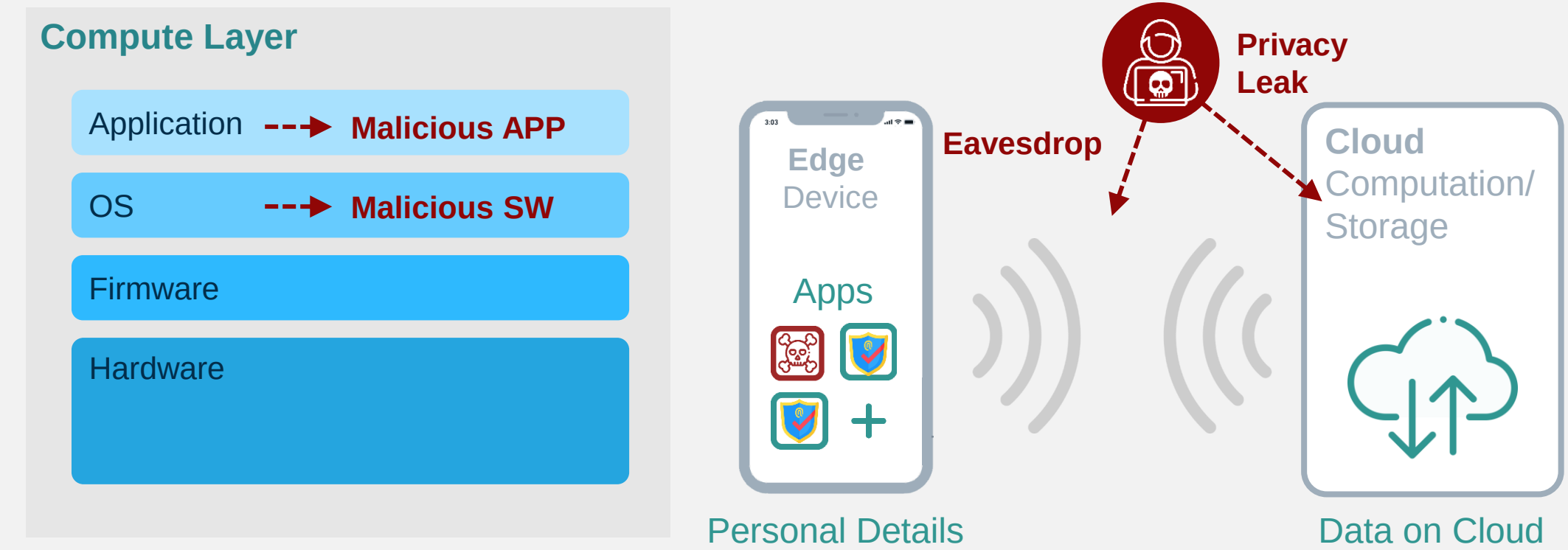
für Oktober 1944

Nr. 00008

	Datum	Walzenlage			Ringstellung			Steckerverbindungen								Kenngruppen			
St	31.	IV	V	I	21	15	16	KL	IT	FQ	HY	XC	NP	VZ	JB	SE	OG	jkm	ogi	ncj	glp
St	30.	IV	II	III	26	14	11	ZN	YO	QB	ER	DK	XU	GP	TV	SJ	LM	ino	udl	nam	lax
St	29.	II	V	IV	19	09	24	ZU	HL	CQ	WM	OA	PY	EB	TR	DN	VI	nci	oid	yhp	nip
St	28.	IV	III	I	03	04	22	YT	BX	CV	ZN	UD	IR	SJ	HW	GA	FQ	zqj	hlg	xky	ebt
St	27.	V	I	IV	20	06	18	KX	GJ	EP	AC	TB	HL	MW	QS	DV	OZ	bvo	sur	ccc	lqe
St	26.	IV	I	V	10	17	01	YV	GT	OQ	WN	FI	SK	LD	RP	MZ	BU	jhx	uuh	giw	ugw

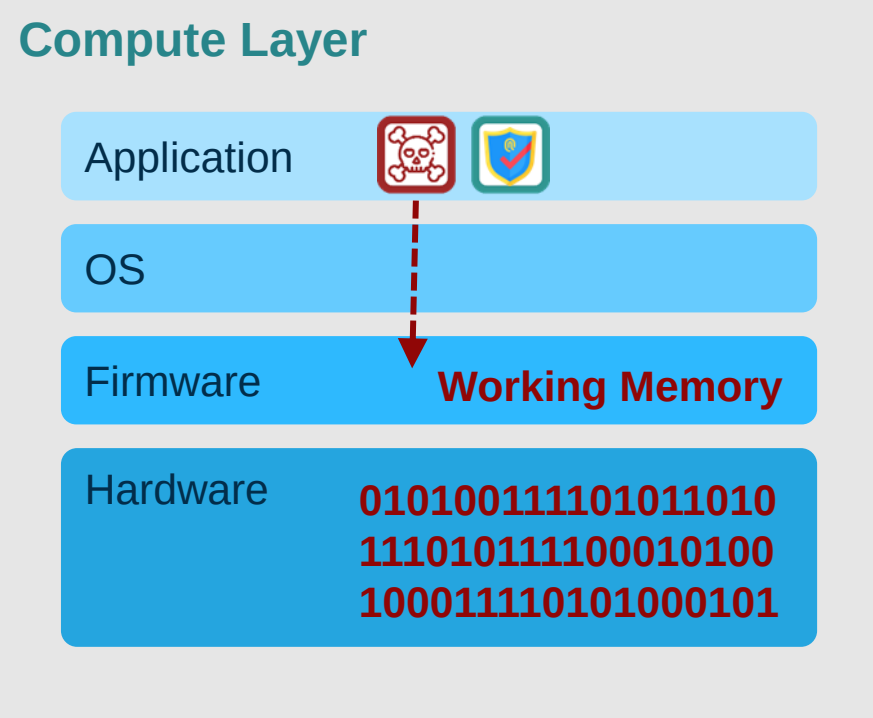
Threats Example – **Malicious Applications**

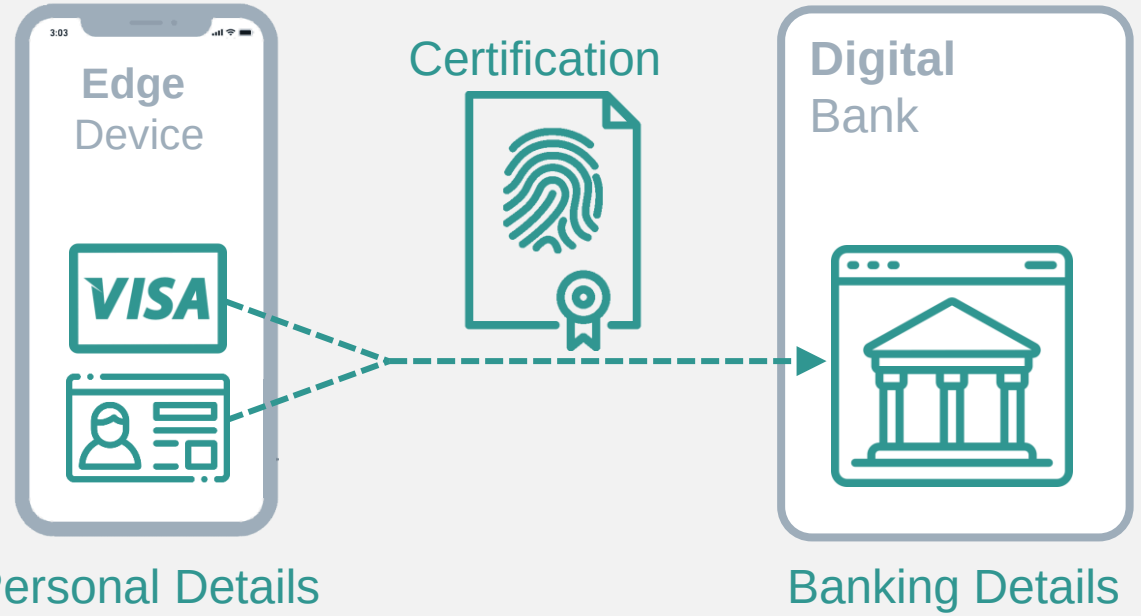
- **Reconfigurable characteristic** provides flexibility for Software Defined Applications
- So, how do we safeguard software from attack when it is continually changing?



Protection Needed to Avoid **Malicious Software**

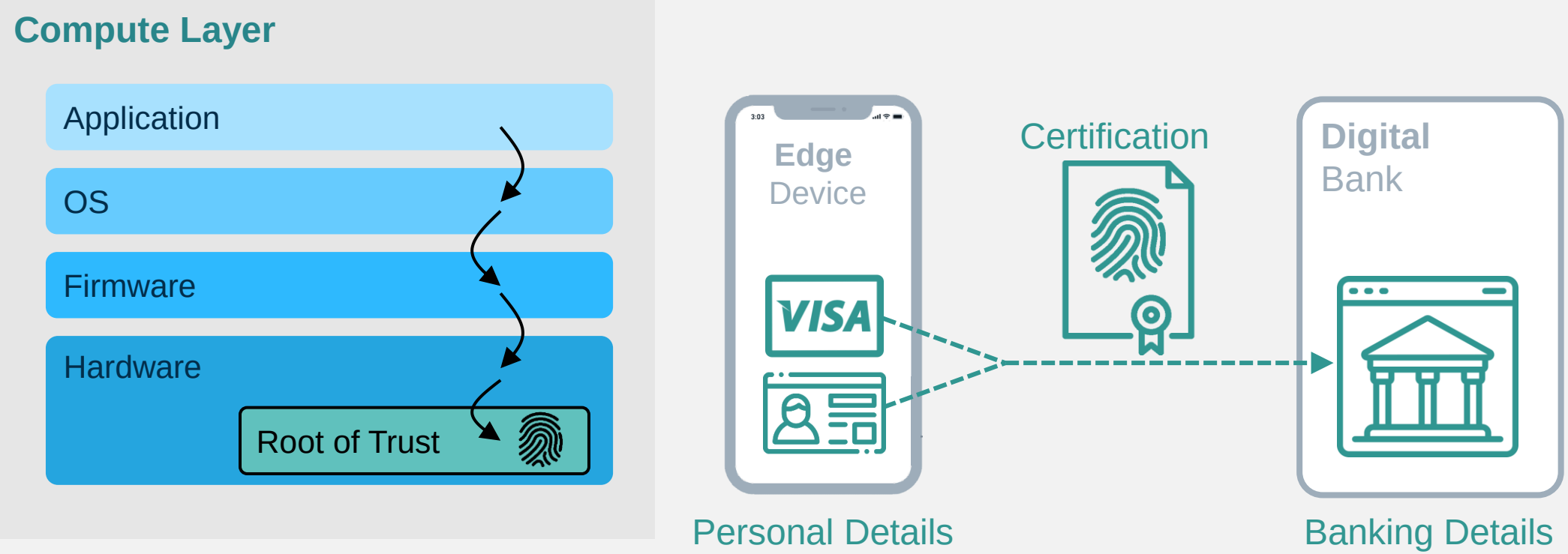
- Need to authenticate software (Integrity) and **protect data-in-use**
- Key for preventing software attack **Isolation and Privilege for Secure Environment**





Protection Needed to guarantee **Authentic Software**

- Need to **authenticate Boot Code and OS (as genuine)** to make sure device starts securely
- Secure boot needs **Hardware Root of Trust, Unique ID, Anti-tampering, and Crypto Engine**



The Foundation of the Security Ecosystem

Software Security Ecosystem
- Continually changing and adapting to new threats
- Relies on immutable Hardware Root of Trust

PUFsecurity
- Hardware Security For the entire lifespan of the Chip
- Foundational **Hardware Root of Trust** for Software

Hardware Root of Trust
is indispensable for…

- Protecting Software and Applications
- Device Registration
- Validating software integrity from initiation
- Providing secure execution environment
- Protecting data in-use & in-transit

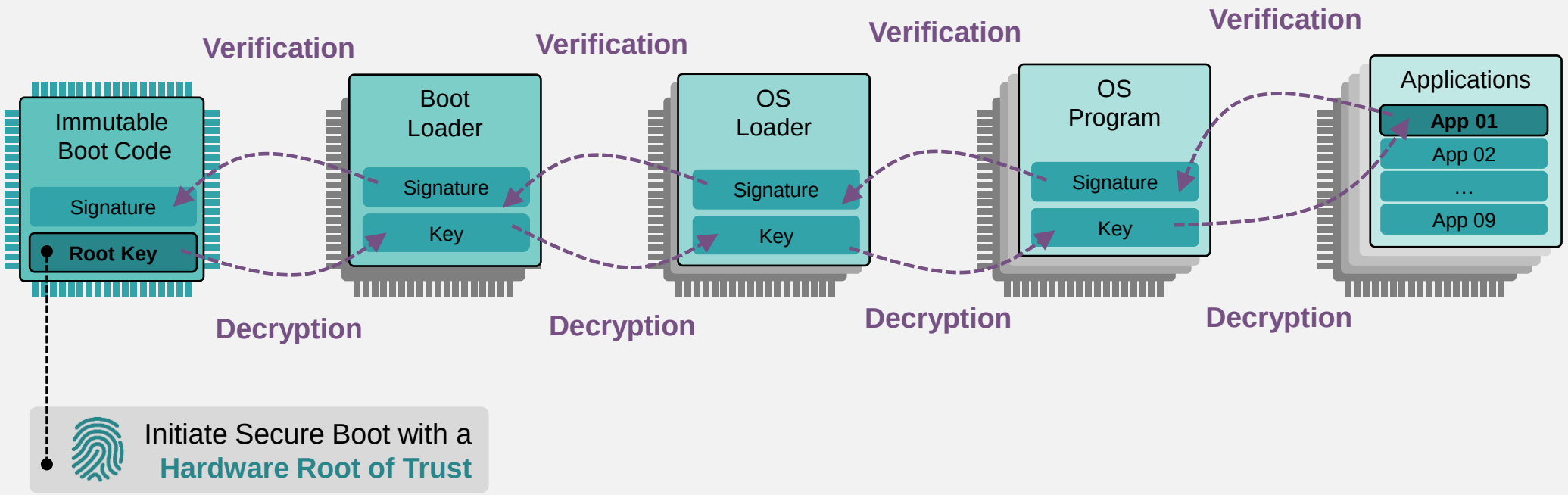
Agenda

1. Cybersecurity Threats & Trends
2. Importance of Hardware Security
3. **Chip Fingerprint**
4. PUFsecurity Solution

Chain of Trust from **Chip Fingerprint**

- **Hardware Root of Trust anchors and protects;** application authentication, data encryption, secure execution environment, SW/FW integrity, certification, identity, and key exposure

The **Secure Boot** Process with Chain of Trust



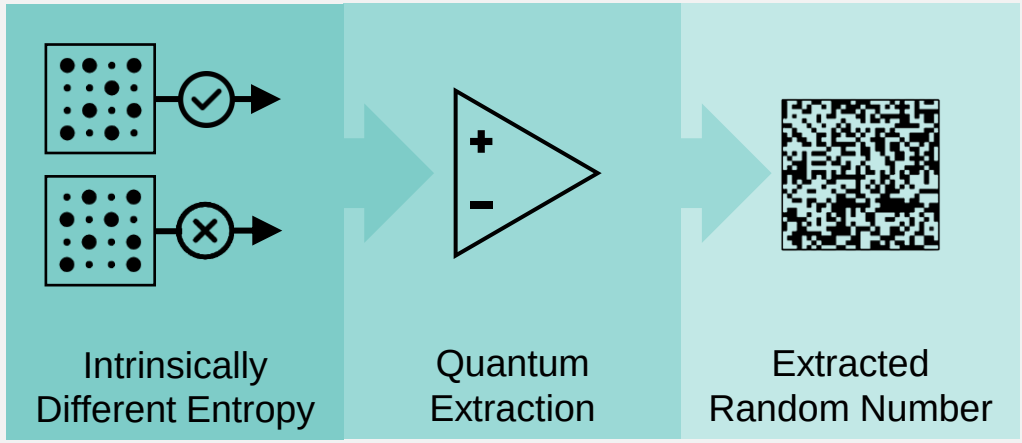
PUF: Physically Unclonable Function

Human Fingerprint
(Biometric)

Collision probability $1/10^{20}$
(12points)

Chip Fingerprint
(Quantum Tunneling PUF)

$2^{64}= 1.8x10^{19}$; $2^{256}=1.5X10^{77}$
$2^{128}= 3.4x10^{38}$; $2^{512}=1.3x10^{154}$



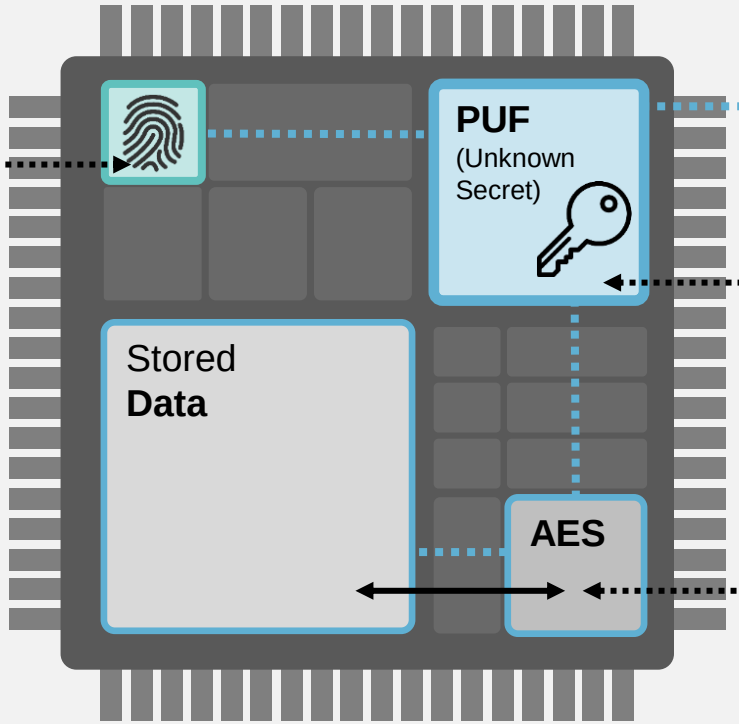
→ 256 bits ID can provide each IC unique identity

What **Chip Fingerprint** can do

- **Unique Identity** – offer unique secret for each chip
- **Unique & Unclonable Identity** – offer decentralized public/private key pair to avoid possibility of Bitcoin theft

UID
(Unique Identity)

- **Inborn PUF UID**
- Cannot be Blank
- Cannot be Clones
- Cannot be Assigned



Shared Key
(Known Secret)

HUK
(Hardware Unique Key)

- **Inborn PUF HUK**
- **Unknown secret key** that never leaves the chip as the foundation for the Secure Ecosystem

External **Data**

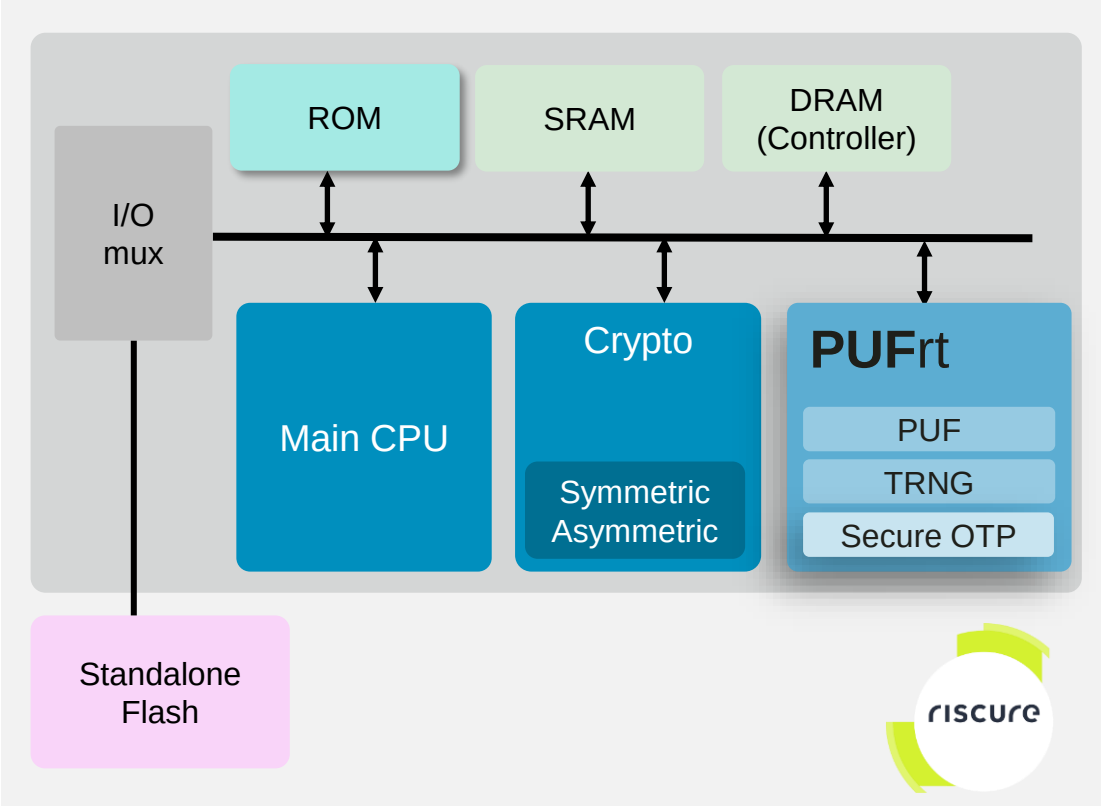
Derived from **Inborn PUF**

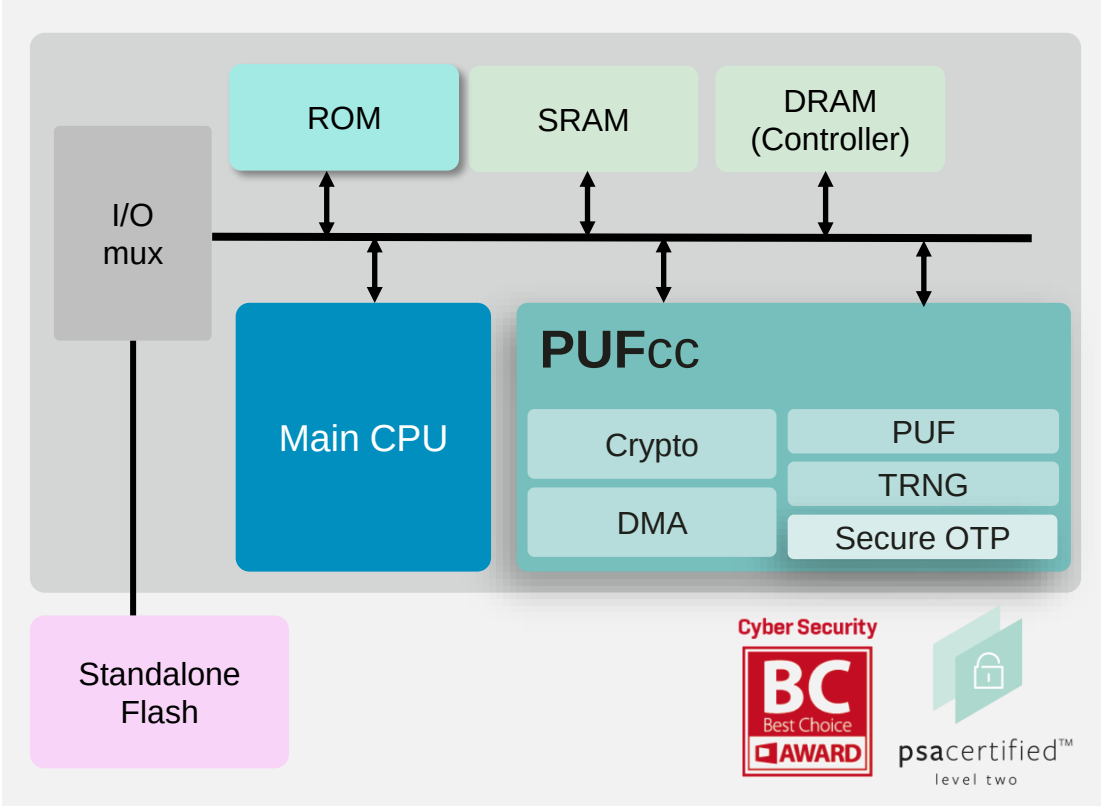
Agenda

1. Cybersecurity Threats & Trends
2. Importance of Hardware Security
3. Chip Fingerprint
4. **PUFsecurity Solution**

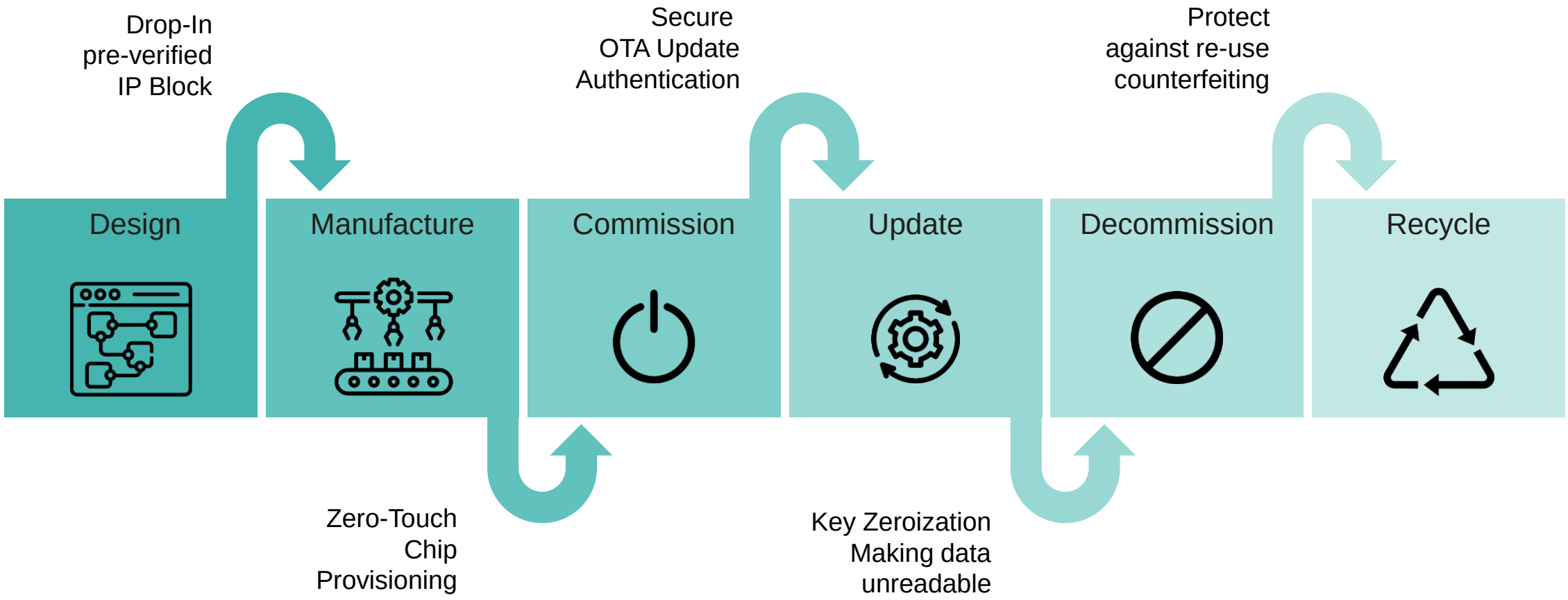
Chip Design **Security Considerations**

- **Riscure & PSA Certificated Level 2 Ready** Security, including Initialization, Secure Storage, Firmware Update, Secure State, Crypto. Support TF-M and Mbed TLS for IoT and Automotive ecosystem

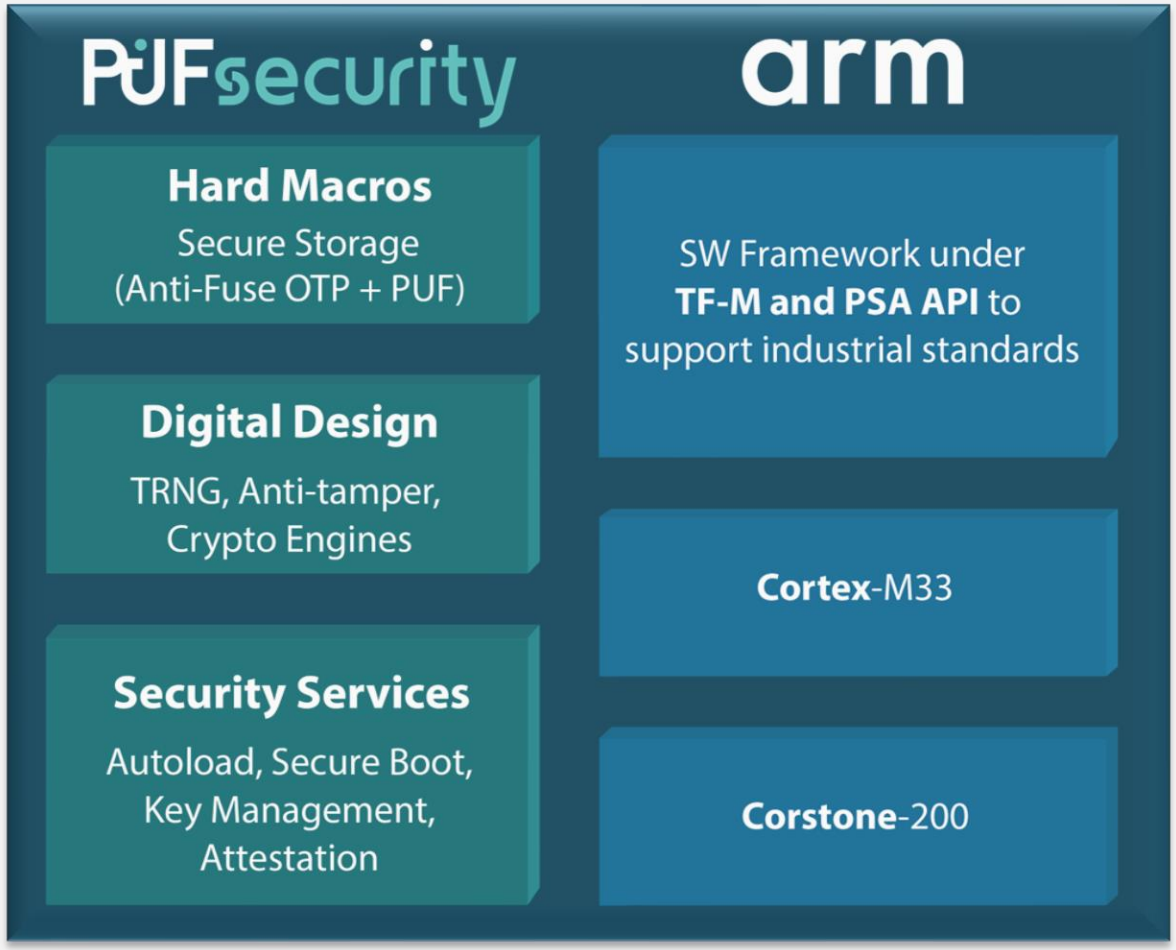




Full **Lifecycle Protection**.



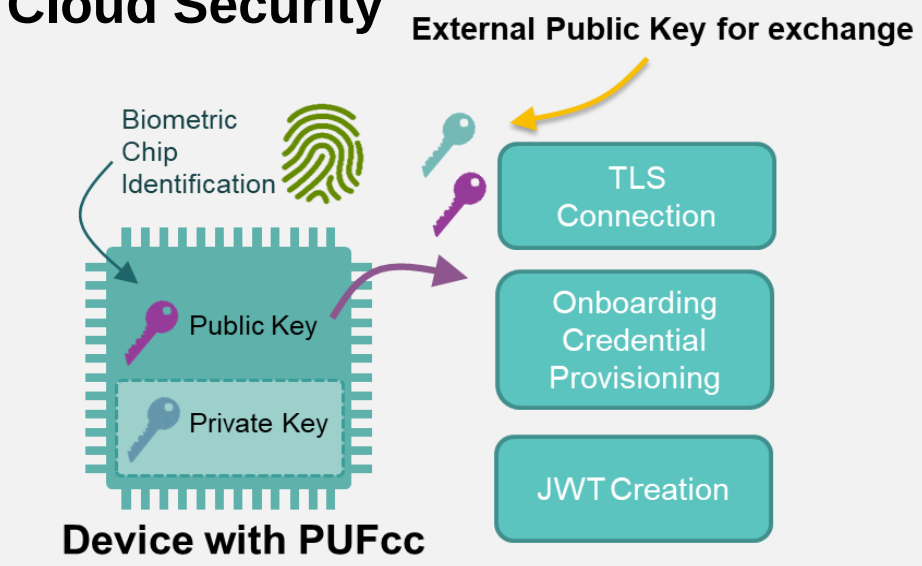
Joint Solution for PSA Certified Level 2 Ready



TLS Compliant Solutions

matter

	PUFcc	PUFcc7
Compliant TLS	TLS 1.2	TLS 1.3 Add SHA3, EdDSA, X 25519/X448, KMAC
Compliant FIPS	FIPS 186-4	FIPS 186-5
Public Key Algorithm Speed Performance	1x	Up to 22x



Summary

Why PUF-based **Hardware Security ?**

Software Security can be vulnerable to cyber attacks as new threats and countermeasures continually emerge.

An immutable **Hardware Root of Trust** is essential for establishing a secure ecosystem from chip to application.

Without **Authentication Prior to Use**, applications and software will remain unable to prove they are genuine.

Secure device entire lifecycle with **PUF-based** inborn **Chip Fingerprint** Solution

Thank you for your time .

PUFsecurity
AN eMemory COMPANY