Aalto University

Saara Matala, Thomas Nyman, N. Asokan

Designing Trust

Historical Insight into the Emergence of Trusted Execution Environment (TEE)

TEE is central to modern mobile platform security. The technology was first widely deployed in Nokia in the early 2000s as an answer to emerging mobile security problems and became an industrial-wide standard.
Understanding the past, helps us to master the technology today and develop it in the future.

Aim and objectives

- To study the emergence and establishment of **mobile TEE** from historical perspective.
- To recognize **key actors**, **critical decisions**, and central **sources of influence**.
- To evaluate contribution of a single company in the creation of a **global industrial standard**.

Research outputs

- **Oral history** collection of 15 interviews: researchers, software developers, managers.
- The mobile TEE emerged as a **technology-driven project** instead of being implemented as a top-down strategic decision.

I. Emergence of Mobile Security

Before the emergence of 3G system, **communication security** was the main concern.

Downloadable applications transformed phones from closed to open systems from the mid-1990s onwards.

→Need to protect the **integrity of the device**

from users and hackers.

- Regulatory interest in **safe storage** for radio frequency parameters.
- Teleoperators' interest in **strong subsidy lock**.

III. Security as Enabler

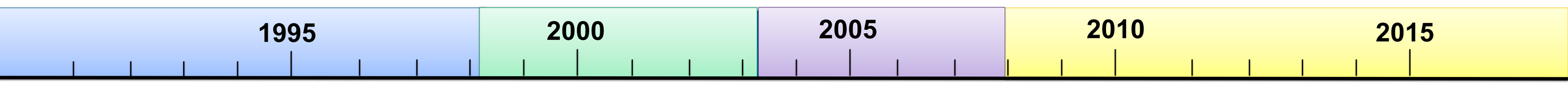
Secure processor environment required coordinated changes in **software** and **hardware** development, and in **manufacturing** process.

→ Cooperation with Texas Instrument and ARM led to commercialization of **hardware-enforced security**.

For the mobile manufacturer, **security was difficult to sell but crucial to have.**

→ Security translated from a problem into an enabler.

- Enhanced protection of **customers business cases** (SIMlock, anti-virus tools, DRM).
- Security certificates for **model variation** in manufacturing.



II. Mobile Platform Security

Trade-off between physically separated secure processing and cost-efficiency.

→ Introduce **secure processor mode** instead of additional physically isolated chip.

BB5 as a milestone towards mobile platform security.

- Organisational culture: From **security through obscurity to security through transparency.**
- Platform design: **Security from an add-on feature to integral in platform architecture**.

IV. Standardized Trust

Active participation in mobile security standardisation forums.

- Ensure emerging standards are **compatible** with Nokia's solution.
- To **facilitate competition** between component suppliers.

2008: TCG: MTM (mobile TPM) 1.0

→ 2014: TPM 2.0 Mobile Specifications.

2010 GlobalPlatform TEE client API.