Towards an Open Framework Leveraging a Trusted Execution Environment

TrustData'13

by
Javier González

Javier González - jgon@itu.dk
Philippe Bonnet - phbo@itu.dk

IT University of Copenhagen

define: privacy

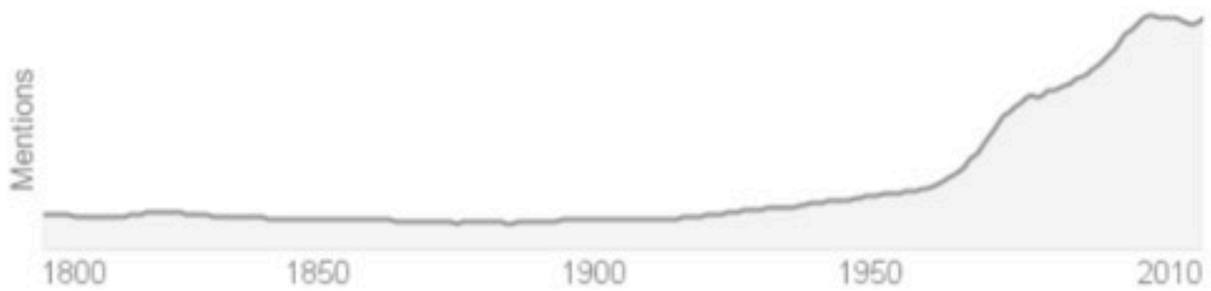
pri·va·cy
/ˈprīvəsē/

noun
noun: **privacy**

1. the state or condition of being free from being observed or disturbed by other people.
   "she returned to the privacy of her own home"
   synonyms: seclusion, solitude, isolation, freedom from disturbance, freedom from interference More
- the state of being free from public attention.
  "a law to restrict newspapers' freedom to invade people's privacy"

Translate privacy to Choose language

Use over time for: privacy



IT University of Copenhagen

Contextual Integrity

Helen Nissenbaum. *Privacy in Context, 2010*

Exchange/sharing of personal data is at the core of any social interaction

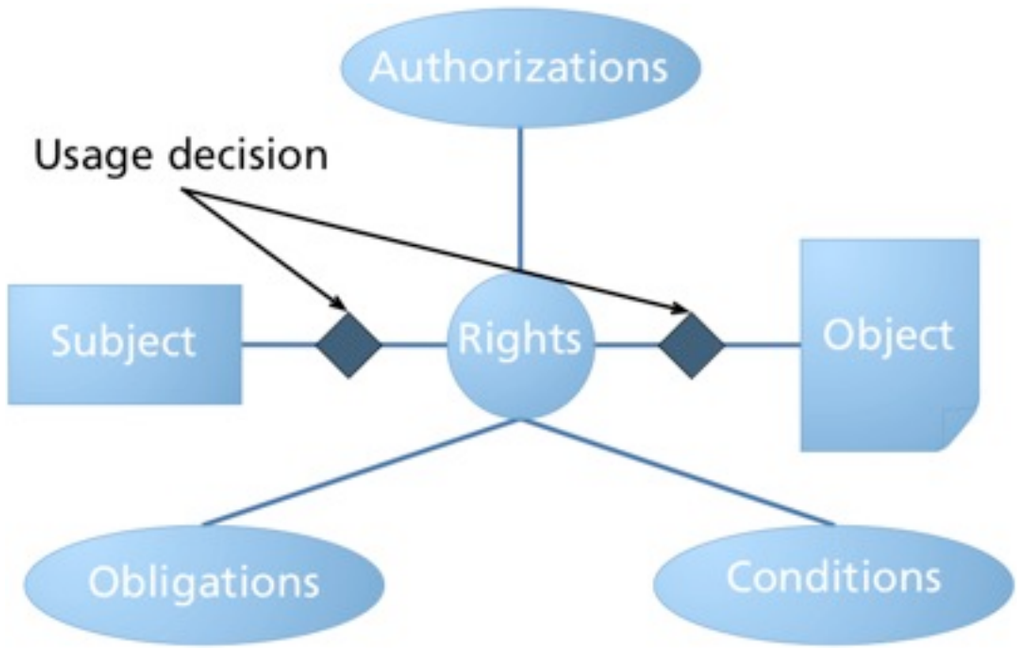
- Privacy is not about "not sharing" personal data!

Any social context (work, education, health, ...) defines – more or less explicitly – a social norm, i.e., an appropriate behavior that is to be expected.

Contextual integrity gives a framework to reason about the norms that apply, in a given social context, to the flows of personal data (i.e., information norms)

IT University of Copenhagen

UCON*ABC*



Formal Model

Strong security Assumptions

No implementation!

Problems:

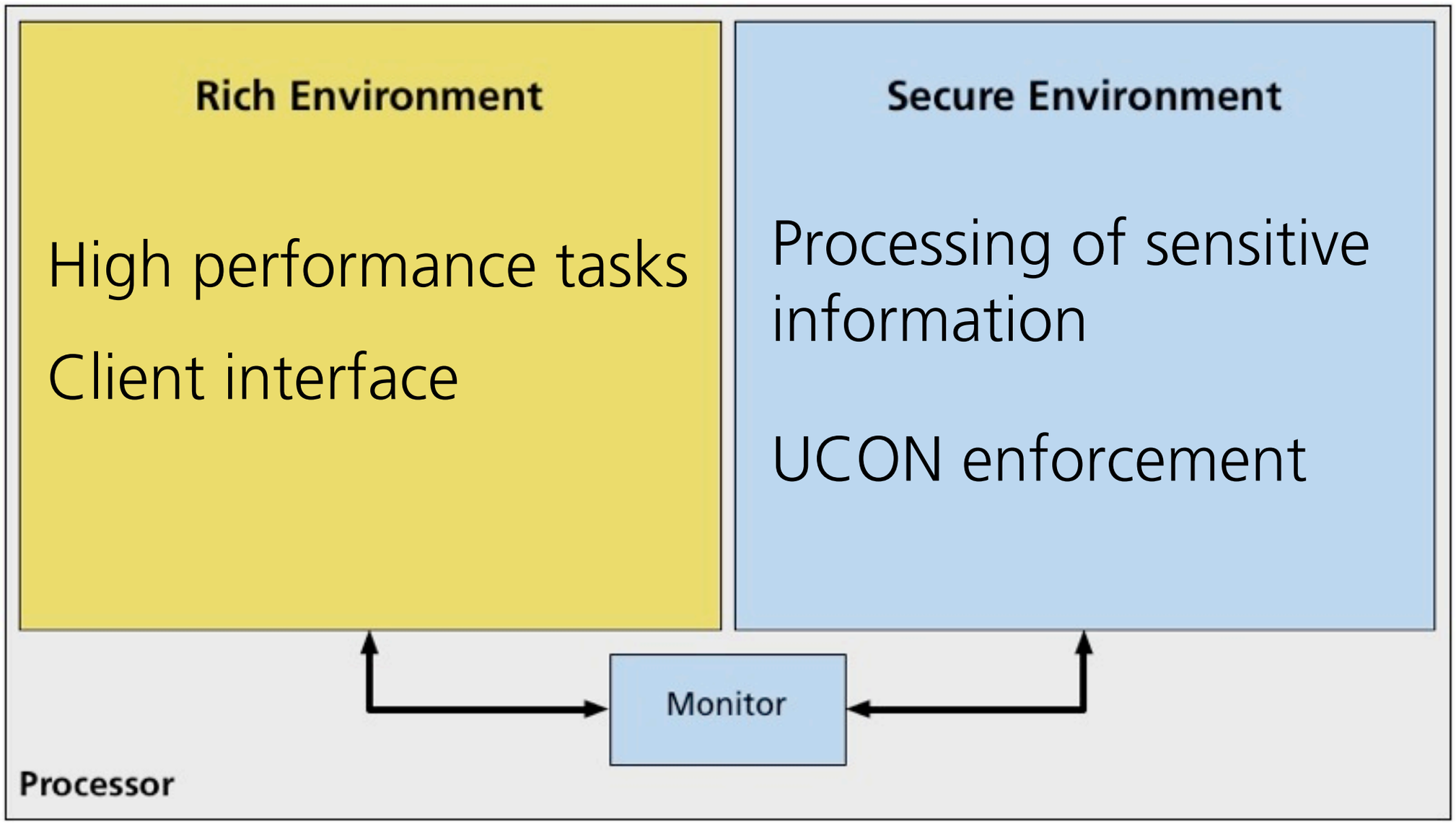
Audit: a posteriori control of how rights were used

Enforcement: a priori control of usage rights

Jaehong Park and Ravi Sandhu. **The UCON*abc* usage control model**. *ACM Trans. Inf. Syst. Secur., 7(1):128–174, February 2004.*

IT University of Copenhagen

Secure / Rich Environment



IT University of Copenhagen

How to organize Usage Control?

Centralized Solutions

Sacrifice security for
innovative applications

Intrinsic security limitations

Decentralized Solutions

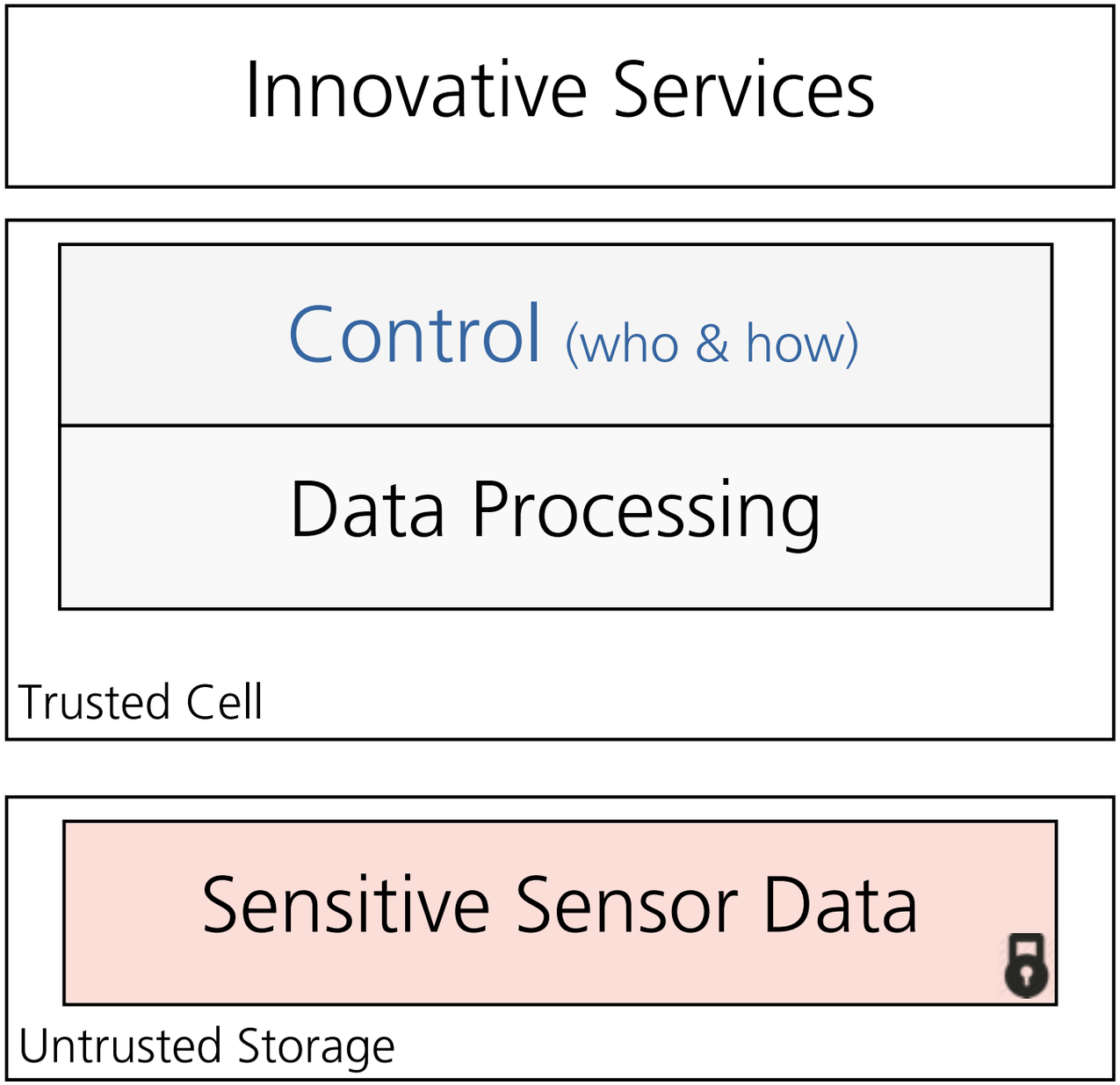
Trade innovative
applications for security

No intrinsic security limitations

No obvious architecture choice

IT University
of Copenhagen

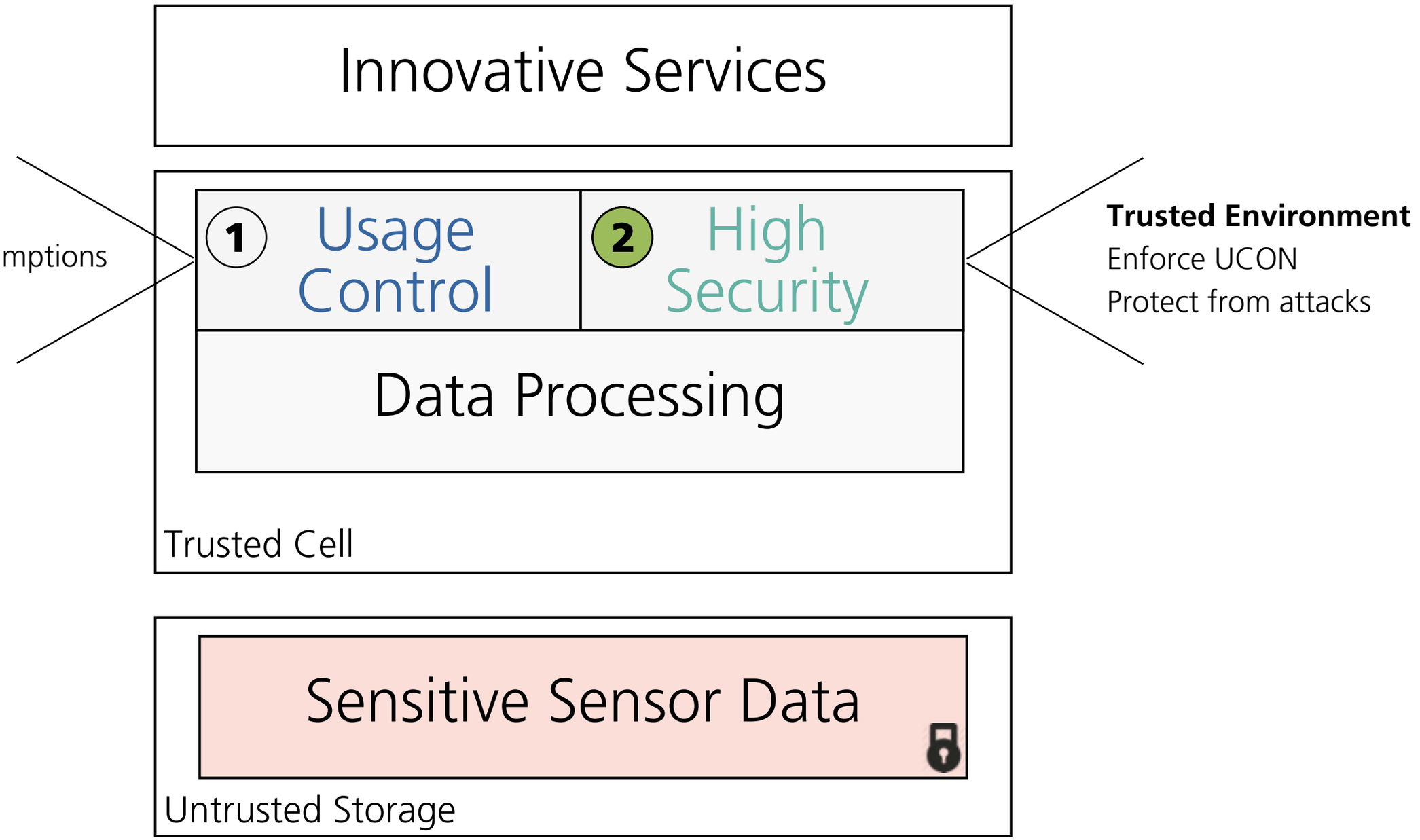
Trusted Cell



Nicolas Anciaux, Philippe Bonnet, Luc Bouganim, Benjamin Nguyen, Iulian Sandu Popa, and Philippe Pucheral. **Trusted cells: A sea change for personal data services**. CIDR, 2013.

IT University of Copenhagen

Trusted Cell

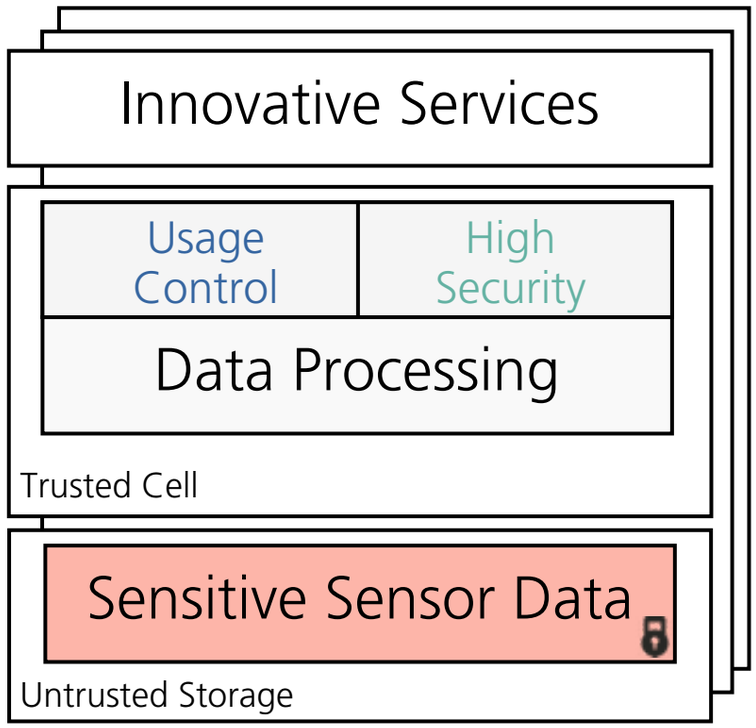


2 TEE: Hardware + Software

IT University of Copenhagen

Secure Platforms

	Level of Protection	Extra Cost	Environment	Examples
Only Software	Low	None	RichOS	Android, Linux, IOS, Windows
Software and Hardware	Medium/High	Low	RichOS + TEE	ARM TrustZone
SW and Tamper resistant HW	Very High	High	Secure Element (TEE)	IBM CryptoCards, ARM SecureCore, Secure Token

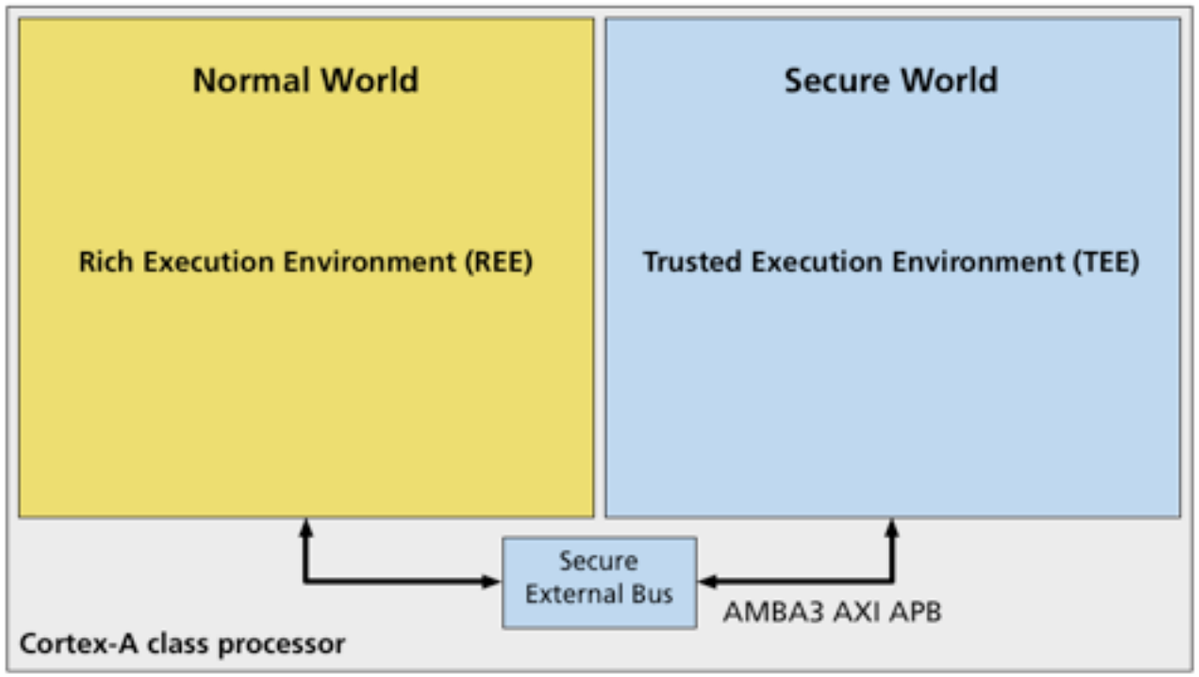


RichOS
+
High Security ⟷ Prevent Class Attacks!!
+
Low Extra Cost

Trade-off

IT University of Copenhagen

ARM TrustZone



Disabled by OEMs

Difficult to verify in a given development board

There is none or little available documentation

TrustZone support today:

Xilinx Zynq-7000 AP SoC ZC702

Nvidia Kayla DevKit (Tegra 3)

ARM Versatile Express.

IT University of Copenhagen

Software for TrustZone

Current Situation

Closed commercial solutions exclusive to *Trusted Logic, Gemalto and Giesecke&Devrient (MobiCore)*

Security level virtually increased through obscurity!!

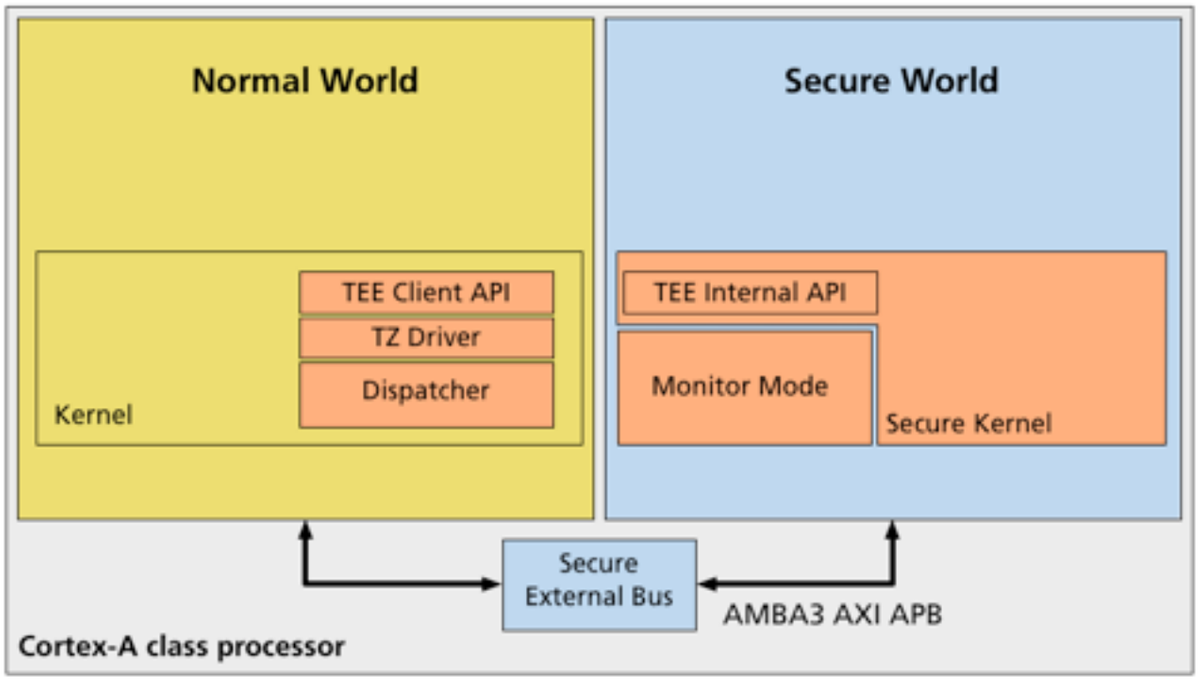
Standard TEE specification by Global Platform and ARM (no implementation)

Happening now

"Open Source" implementation of Global Platform's TEE for ARM TrustZone

Xilinx showing interest in TrustZone

Open Virtualization



Open Source TEE impl.
Support for OpenSSL
Support for standard libraries

Early Implementation
Second fiddle
No standard functions
↪ malloc → TEE_malloc

IT University of Copenhagen

Towards an open TEE

Assembling

Commercially Available Hardware

Xilinx Zynq-7000 AP Soc ZC702

Available Open Source Software

Open Virtualization

Trigger IP Blocks revision

ZC702 tuning

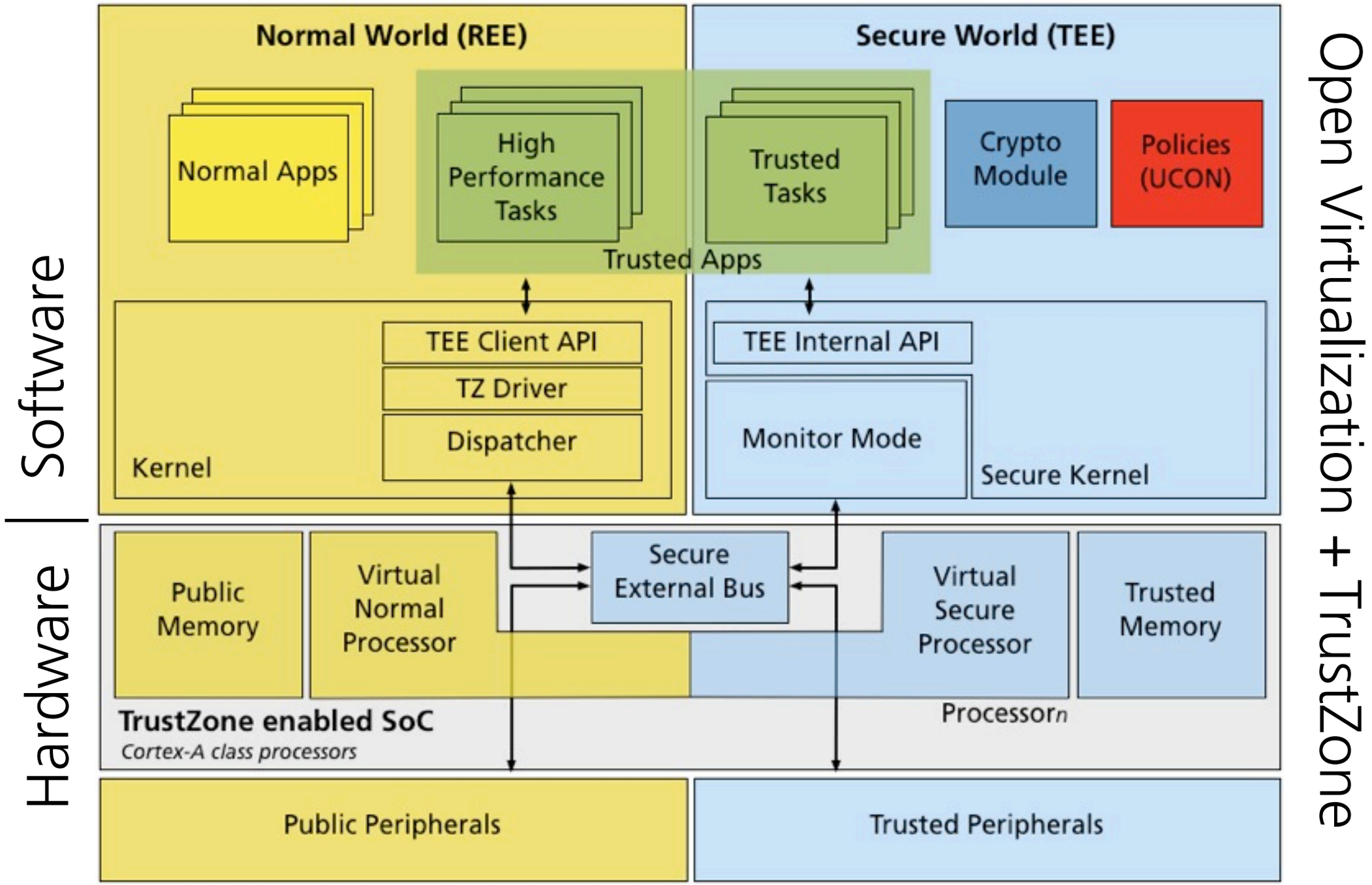
*Distribution via git repository **

Contribution

Complete Documentation

*Wiki for Xilinx ZC702 with TrustZone **

Trusted Cell Design



IT University of Copenhagen

Contributions

Pushing towards a TEE (HW + SW) that is open and available to the research community - currently TEEs are closed, monopolized and obscure.

Trusted Cells: Established formal usage control model (UCON*ABC*) + commercially available and cheap secure platform (Xilinx - ARM TrustZone) + open source implementation of Global Platform's TEE (Open Virtualization).

Roadmap for a decentralized, trusted data platform implementing a Usage Control model while supporting innovative services for big sensor data - the Servfos case study.

IT University of Copenhagen

Towards an Open Framework Leveraging a Trusted Execution Environment

TrustData'13

by
Javier González

Javier González - jgon@itu.dk
Philippe Bonnet - phbo@itu.dk

IT University of Copenhagen