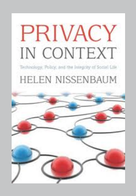
Trusted Cells: Architecture

by
Javier González

Trusted Cells: a decentralized data platform based on Trusted Execution Environments (TEE) embedded on personal data devices (set top boxes, smart phones or smart meters) at the edges of the Internet.

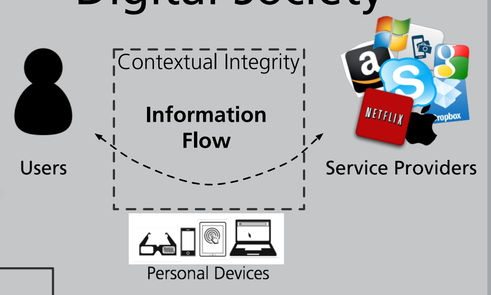
TRUSTED CELL - CONTEXT

Contextual Integrity



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

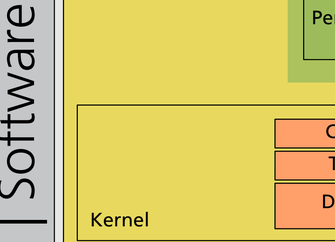
Digital Society

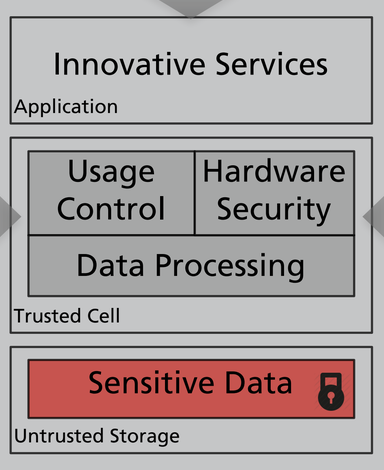


UCON$_{ABC}$

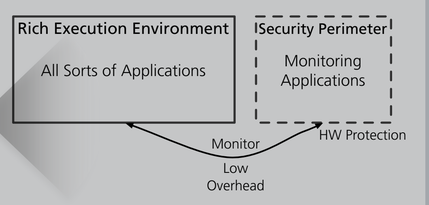
Audit: a posteriori control of how rights were used

Enforcement: a priori control of usage rights





Secure Platforms



	Level of protection	Comm. Abstraction	Execution Env.	Examples
Only Software	Low	Msg, Sockets, SM	Rich OS	Android, Linux iOS, Windows
Software Hardware	Medium High	Shared Memory	Rich OS + TEE	ARM TrustZone
SW + Tamper Resistant HW	Very High	Narrow Interfaces	Secure ad-hoc OS	IBM CC, TPM, Secure Token

Characteristics:

UCON is a formal model (algebra)

UCON can model complex policies: Access Control Lists, Digital Right Management, or Usage Control Policies.

UCON is a perfect candidate to model Contextual Integrity

UCON is founded on very strong security assumptions

There is no implementation!

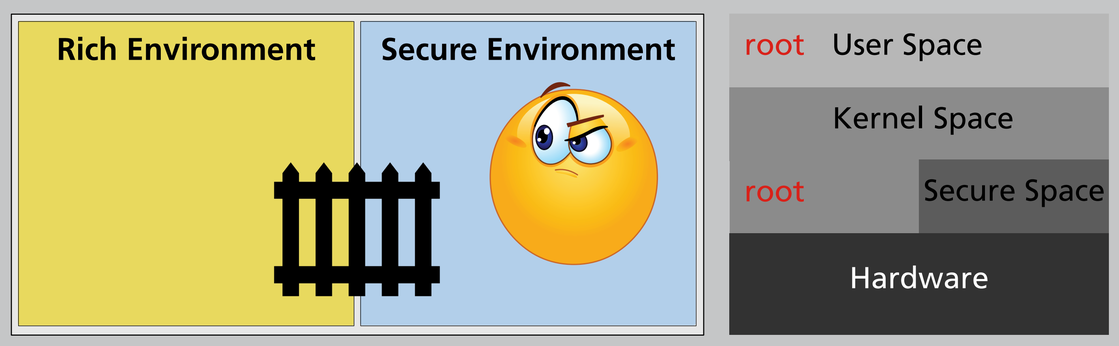
Requirements:

UCON needs to be implemented within a security perimeter protected by hardware so that attackers with root privileges cannot disable it using software.

From inside the security perimeter it should be possible to "monitor" programs outside the security perimeter

Communicating with programs in the security perimeter should entail a low overhead

TRUSTED EXECUTION ENVIRONMENT (TEE) - FRAMEWORK

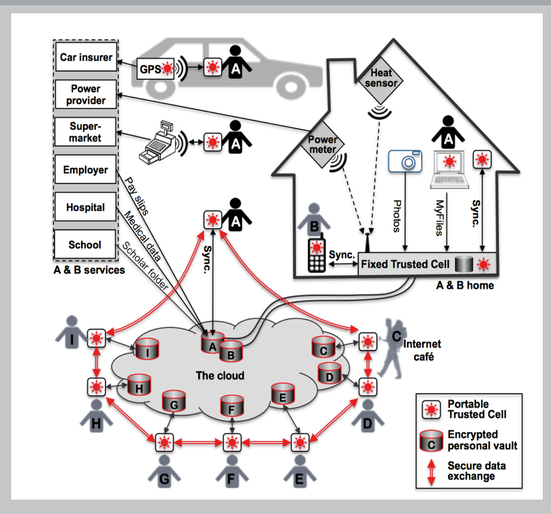


Principle 1: Self preservation first. Under the suspicion of a threat, the secure environment isolates itself logically and gives up availability in order to protect data integrity, confidentiality and durability.

Principle 2: Lead all communications. The secure environment defines all parameters that define this communication: protocol, certificates, encryption keys, etc.

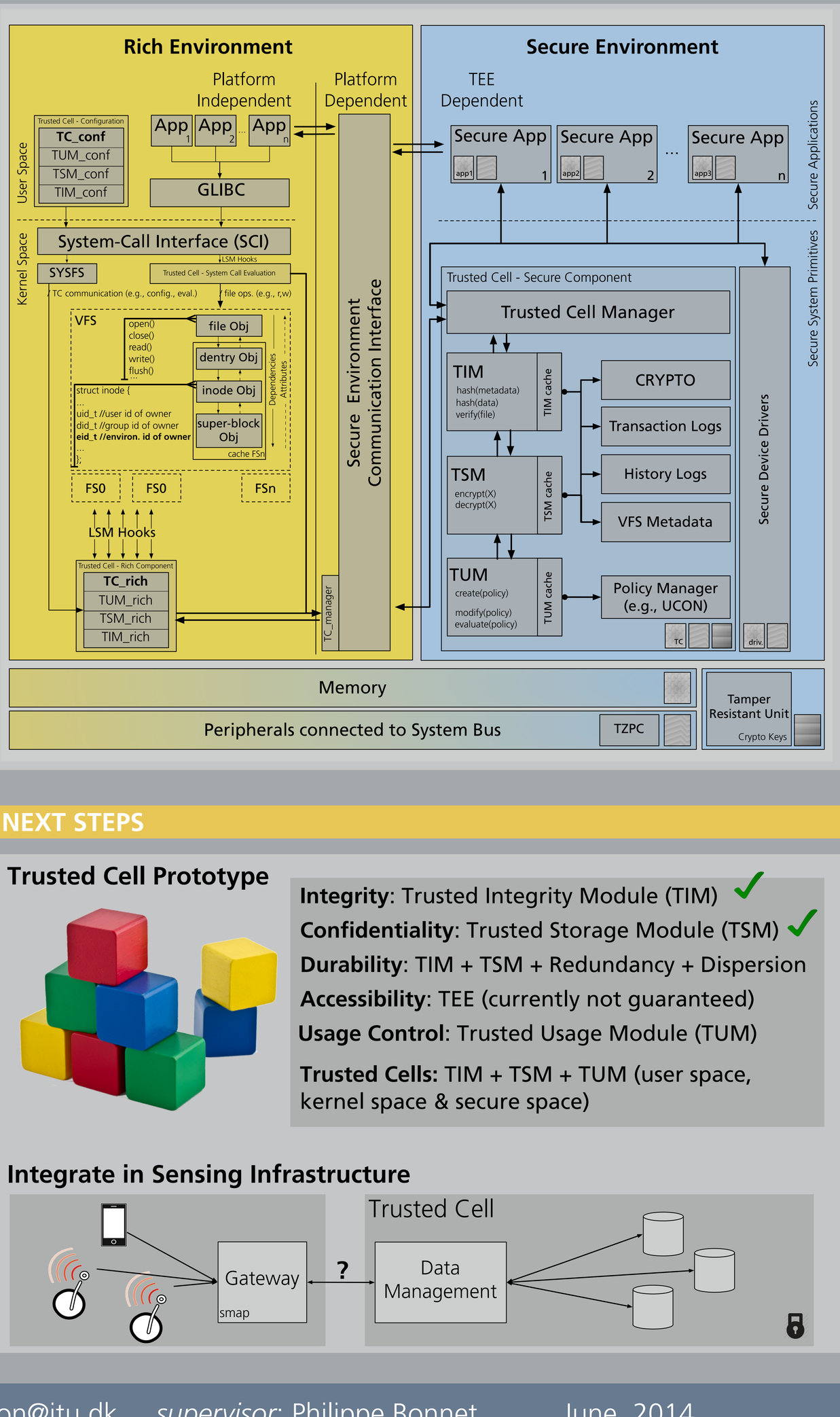
Principle 3: Secure all interactions. The secure area has priority to obtain exclusive access to secure peripherals.

TRUSTED CELL - VISION



Alice (A) and Bob (B) are equipped with fixed and portable trusted cells, acquiring data from several data sources, synchronizing with their encrypted personal digital space on the cloud. Charlie (C) is travelling around the world and can securely access all his data from any (unsecure) terminal thanks to his portable trusted cell. All users equipped with trusted cells can securely share their encrypted data through the cloud.

ARCHITECTURE - LINUX KERNEL



NEXT STEPS

Trusted Cell Prototype

Integrity: Trusted Integrity Module (TIM) ✓
Confidentiality: Trusted Storage Module (TSM) ✓
Durability: TIM + TSM + Redundancy + Dispersion
Accessibility: TEE (currently not guaranteed)
Usage Control: Trusted Usage Module (TUM)

Trusted Cells: TIM + TSM + TUM (user space, kernel space & secure space)

Integrate in Sensing Infrastructure

IT UNIVERSITY OF COPENHAGEN Javier González - jgon@itu.dk *supervisor*: Philippe Bonnet June, 2014