# Usable Hardware Security For Android on ARM Devices


14th February 2012
Jon Geater, Director of Technology

# About ARM

**Founded in November 1990**
- **Spun out of Acorn Computers**

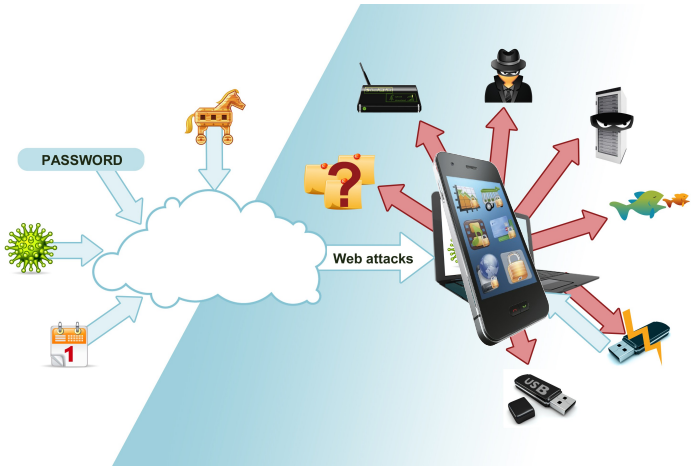
**Designs the ARM® RISC processor cores and GPUs**
**Licenses ARM designs to semiconductor partners who fabricate chips and sell to their customers.**
**Consumer devices are driving industry growth**
- **Smartphones, Tablets, Connected TVs**

Chair the GlobalPlatform Device Committee TEE API Working Group

# PC Threat landscape

# PC Threat landscape

# Coming to Connected Devices Near You




**"An increasing amount of mobile malware has been reported over the past several years, which raises concerns for the future, particularly when coupled with the recent trend towards establishing a more open system environment for cellular handheld devices."**

**NIST Guidelines on Cell Phone and PDA Security**
**http://csrc.nist.gov/publications/nistpubs/800-124/SP800-124.pdf**

The mobile device is fast becoming the centre of our connected lives:

- Capable business devices
- Shopping, banking
- Social networking

PC-like threats are starting to surface:

- Trojans, viruses
- Keyloggers
- Patch cycles

And remember this isn't just phones

# Not Just Phones



# Driving Factors For Change

**3rd era devices bring mobility, consumption and interaction**

**Mobile devices are driving operating system innovation**

- **Moving away from traditional PC/laptop**

**Basis for application and service innovation**

- **Hundreds of thousands of applications developed specifically for mobile**

**Further services limited by risk not device capability**

**Priority now turning to securing people's digital world**

# Traditional Approach

# Traditional Approach

# Traditional Approach

# Is There A Better Way?

# TrustZone

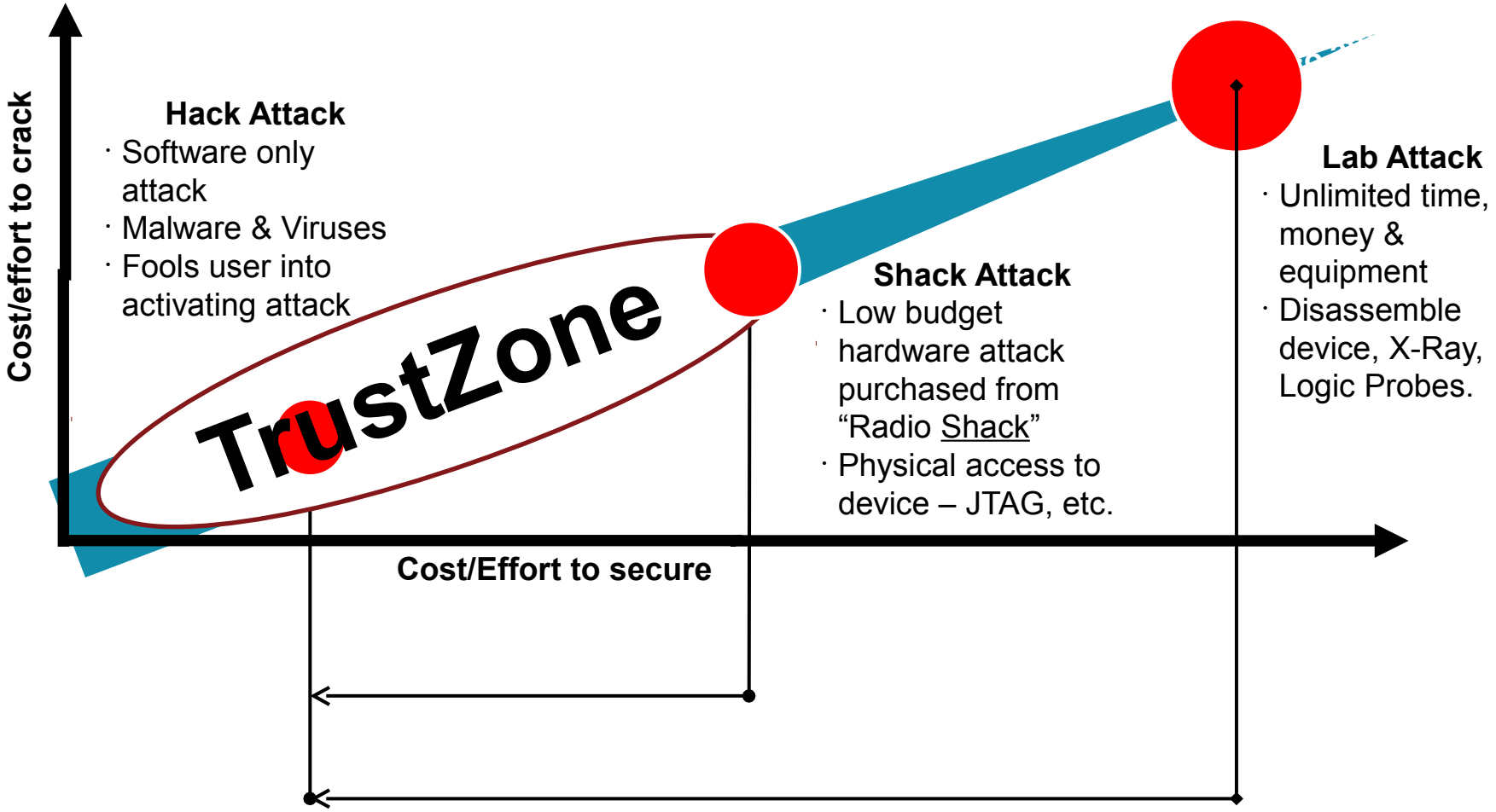
+


GLOBALPLATFORM
THE STANDARD FOR SMART CARD INFRASTRUCTURE

TrustZone®
System Security by ARM

# What is ARM TrustZone?

# Security: A Hacker's Perspective



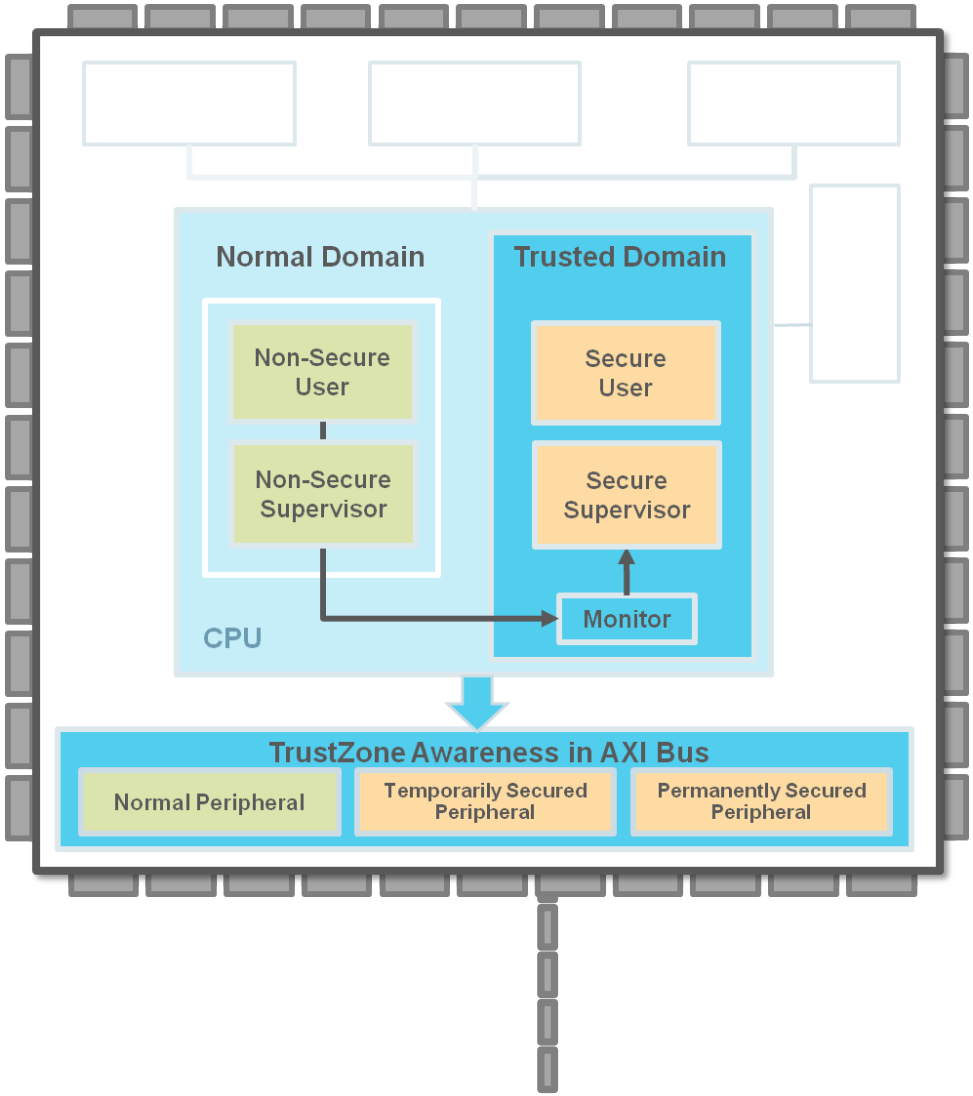

***Knowledge gained from Shack & Lab attacks are frequently used to create Hack Attacks***

# What is TrustZone?

**Appears like a separate security processor, can be treated as a black box device just like a Secure Element or GPU...**

**Key advantages over separate secure processor solutions:**

- **CPU MHz/resources are dynamically shared according to demands**
- **The two isolated domains are implemented in the same machine with no duplication of hardware**
- **Simpler and more flexible platform designs, lower costs and high power/performance efficiency**

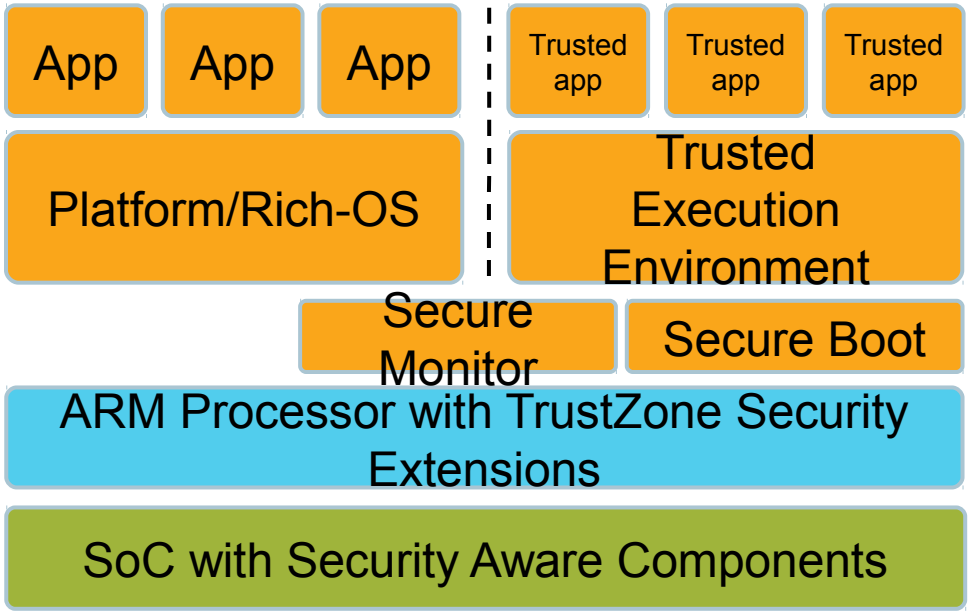


# TrustZone Technology

**TrustZone® technology provides a Trusted Execution Environment (TEE)**

**Eliminates software attack from open/rich OS**

**Delivers two separate domains, normal and trusted**




- Extends across entire system
- Beyond simply the processor
- Delivers secure processing and peripherals

# Extending System Security

**Trusted Execution Environment (TEE) - based on TrustZone technology**

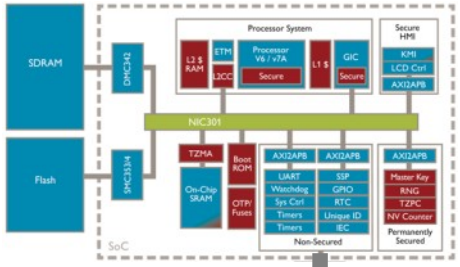
- Defends against software and non-invasive physical attacks
- Enables close interworking with rich OS – fast switching and data interoperability
- Tight integration with peripherals for PIN entry & LCD response

**Secure Execution Environment (SEE) – based on Secure Element**

- Defends against physical attacks
- Enables electronic wallet for primary keys and non-volatile storage of data

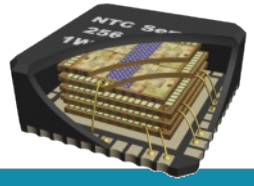
**Some designs TEE coupled with SEE**

- Poor availability of non-volatile memory at <65nm geometries
- Secure Element optimally stacked-die or within same package
  - e.g. 28nm apps processor with 90nm SE bonded on top
  - Enables long term storage of personal user data ($$$, DRM rights, etc)
- Secure Element may be connected to TrustZone Secure World or Non-Secure domain (via encrypted link) depending on system reuse requirements
- Secure Element is not equivalent to SIM/UICC as these are owned by network operator – fragmented s/w and systems




**28nm Apps Processor**

**Secure Element inc SC000**



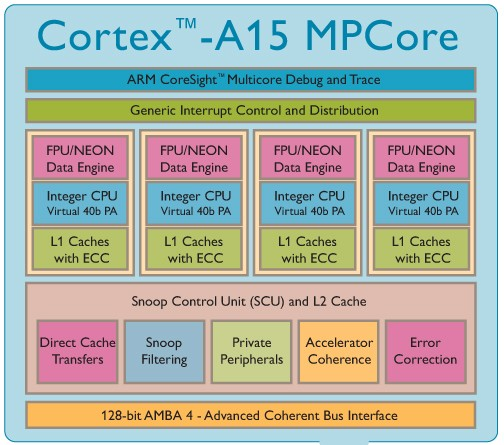
**90nm NV Memory**

# TrustZone Enabled Processors

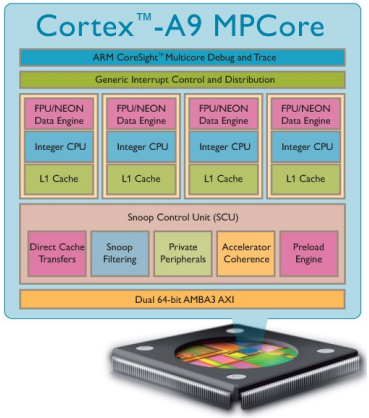
**TrustZone techniology introduced in ARM1176™ processor**
**Standard technology in all Cortex™-A processors**

- **Cortex-A8**
- **Cortex-A9 & Cortex-A5 MPCore™**
- **Cortex-A15 MPCore**

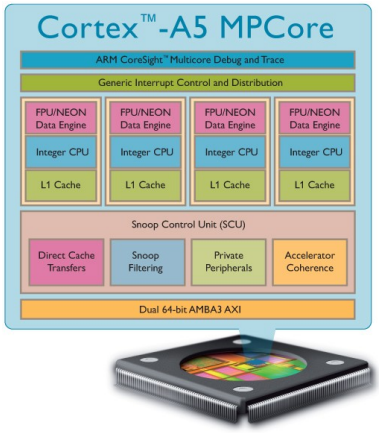
**TrustZone technology is baked into the DNA of all application processors**
**Systemic approach to security which extends from the processor to entire memory and peripheral systems**



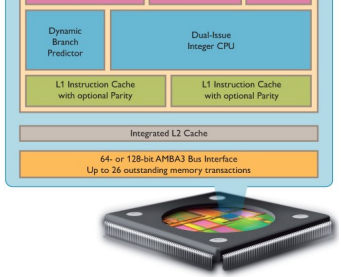

Cortex-A15



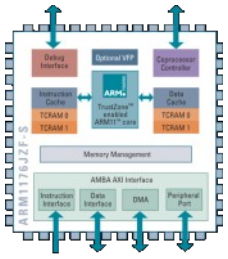

Cortex-A9




Cortex-A5




Cortex-A8



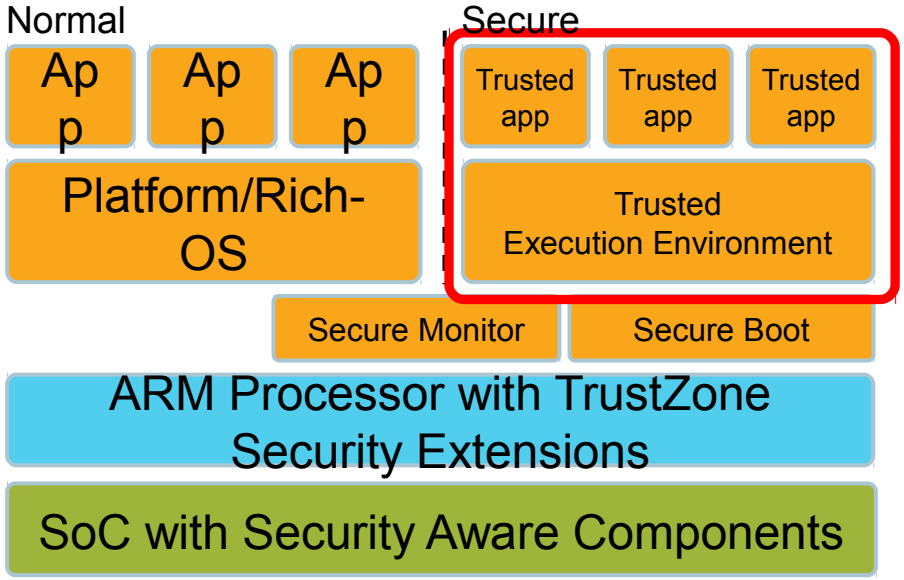

ARM1176

# TrustZone Technology Summary

**TrustZone technology provides a Trusted Execution Environment (TEE)**

**Eliminates software attack from open/rich OS**

**Delivers two separate domains, normal and trusted**




- Extends across entire system
- Beyond simply the processor
- Delivers secure processing and peripherals

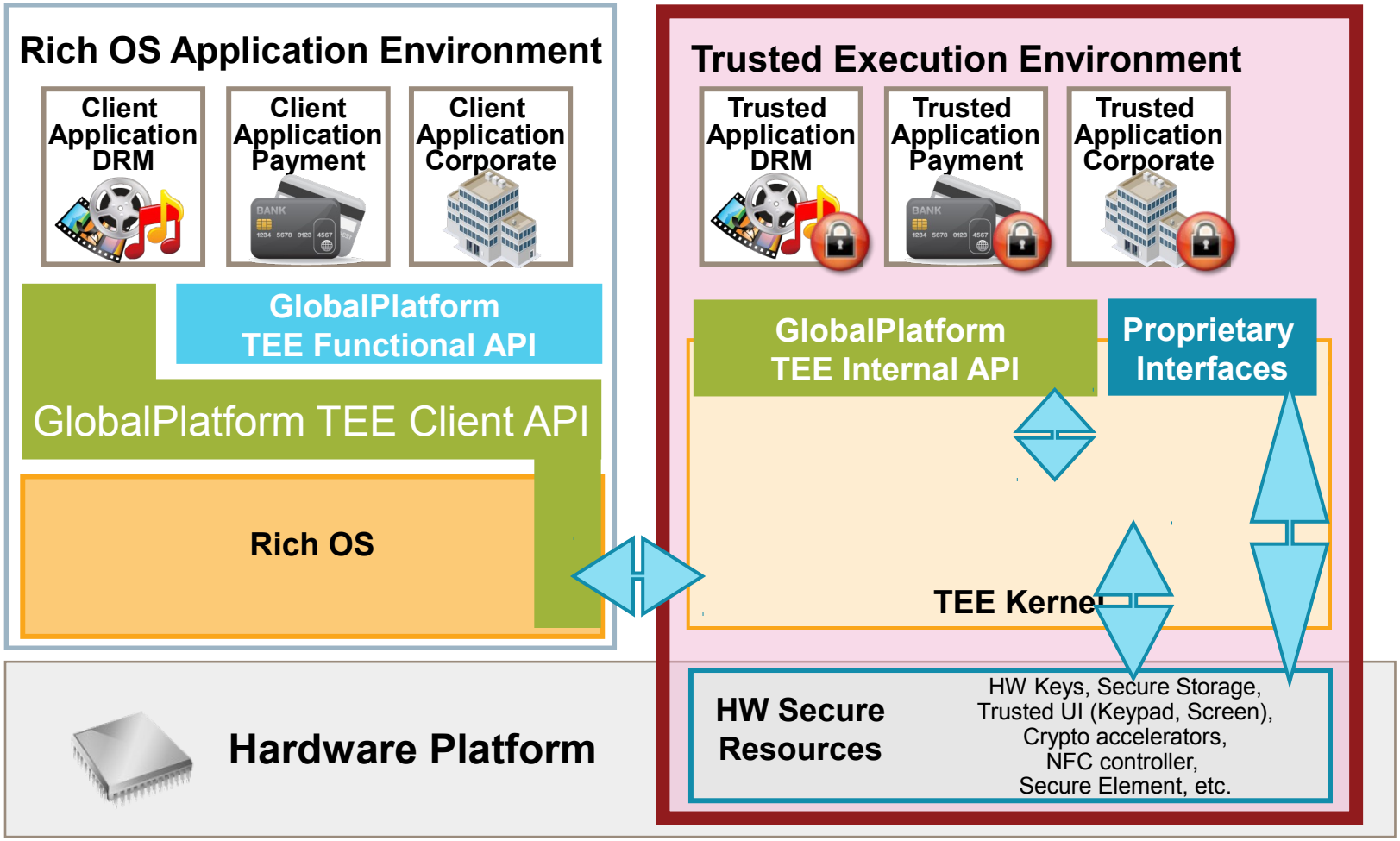
- TEE provides scalable environment for security applications
  - Content management, strong user authenticated payments, etc.

# Security: A System Perspective


- Security is a whole system game
- Today's systems are large, complex, diverse and increasingly online
- Information and processes are key assets to protect
- Protecting this information means implementing strong, consistent security standards on many different technology platforms

# Remember the Traditional Approach?

# GlobalPlatform Defining TEE Standards




GlobalPlatform Standards Status :

Done

Future Development

# Benefits of the Standardized TEE

**Consistency**

**Choice**

**Scale and future-proofing**

**Secure application ecosystem**

**Multi use-case**

**Broader talent pool**

**Device makers don’t have to build it themselves**

# Usable Security

**Note that these are *possible, example* use cases. The solutions are not necessarily in the market today.**

# How Hard is it to Checkout a T-shirt?

15s

32

59s

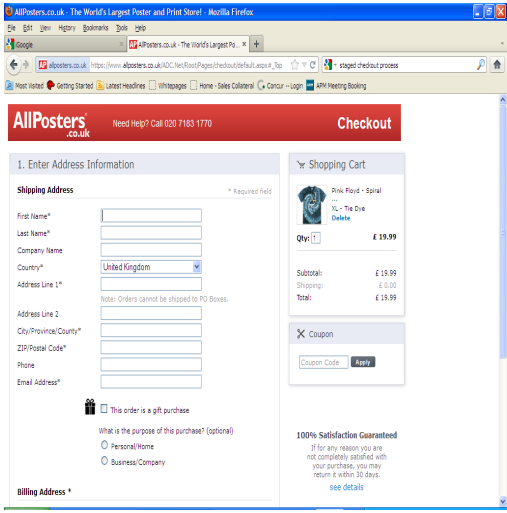
56

78s

23

7s

9




**TOTAL**
**2 minutes 29 seconds**
**120 keystrokes**

***Is this better or worse on a touchscreen tablet?***

# Enhancing the Experience with TEE

TrustZone® System Security by ARM

2s

4

TrustZone® System Security by ARM

1s

1

TrustZone® System Security by ARM

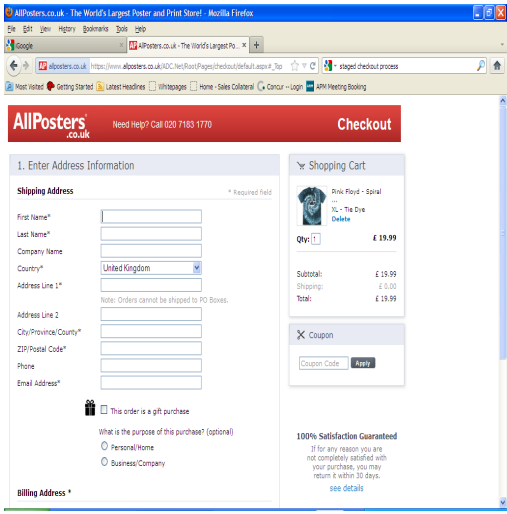
0s

0

TrustZone® System Security by ARM

0s

0




**TOTAL**
**3 seconds**
**5 keystrokes**

# Example Enterprise Use Cases

## Seamless network authentication

Currently the preserve of expensive and complicated systems with laptops and TPMs, TrustZone/TEE bring strong, no-touch network authentication to mobile allowing seamless, secure access to internal network resources.

- ✓Added security
- ✓Added convenience
- ✓Added productivity
- ✓Cost savings

# Example Enterprise Use Cases

## Secure documents on the go


Using secure device ID, VPN/ERM and trusted display, secure document handling becomes possible. Essential for sensitive documents such as financials and medical records.

- ✓Added security
- ✓Added convenience
- ✓Added productivity
- ✓Cost savings

# Example Enterprise Use Cases

## Embrace Cloud with access *anywhere*

ombining high-speed network connections
ith strong ID and login capabilities,
ocument protection and policy processing
akes mobile devices the ideal window to
oud services on the move.

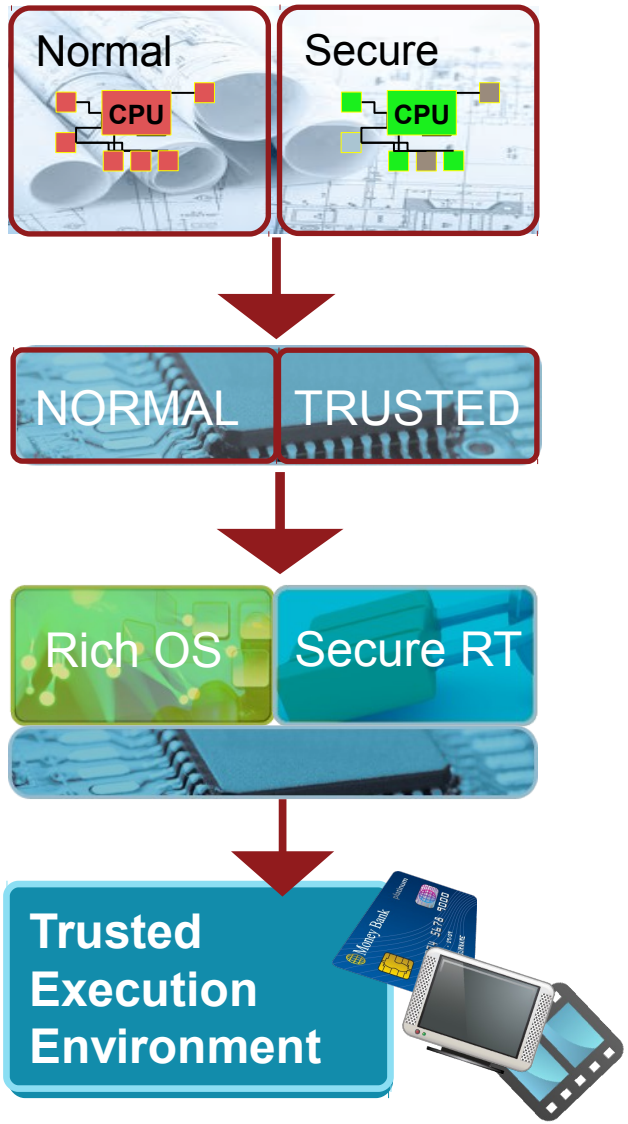
- ✓Added security
- ✓Added convenience
- ✓Added productivity
- ✓Cost savings

# Those Were All Security Use Cases, But They All Make Life Easier

**Note that these are *possible, example* use cases. The solutions are not necessarily in the market today.**

# Summary

# 3 Steps To Usable Security




TrustZone provides a trusted area in the CPU that is protected from normal software attacks

- Combats unwanted rooting, viruses and Trojan attacks for critical services.
- But at the same time embraces innovation on the open application side

Trusted boot and secure runtime ensure platform integrity.

Standardization

- The TEE working group in GlobalPlatform and is working hard to standardize access to this space to bring consistent security, trust and application environments to connected devices

GLOBALPLATFORM
THE STANDARD FOR SMART CARD INFRASTRUCTURE

# What Can You Do?

**Talk to us about security platforms**

**Consider adopting a standardized TEE approach**

**Talk to your suppliers**

**Get involved!**

# Additional Information

**trustzone@arm.com**

**GlobalPlatform:**

**The Trusted Execution Environment:**

**Delivering Enhanced Security at a Lower Cost to the Mobile Market**

**http://www.globalplatform.org/documents/GlobalPlatform_TEE_White_Paper_**

# Questions?