FIDO & TEE: Simpler, Stronger, Authentication

Rob Coombs - Security Marketing Director
Agenda

- Introduction
- Four Compartment Security Model
- Emerging Trends
  - Trusted Apps
  - FIDO – Moving beyond passwords
- Summary
Security & Trust

- Two lenses to look at Security & Trust with:
  - Protection against threats
  - Delivering better user experiences
- Computational Trust builds on strong authentication of users and devices
PC Era Authentication: Pockets Full of Hardware
Applying Lessons to Modern Mobile Security

- Hypervisor (with hardware support) separating large pieces of code
- Small, certifiable Trusted Execution Environment inside Application processor isolated using ARM TrustZone® technology protecting against software attacks
- Secure Element for tamper proof security
TrustZone Based Trusted Execution Environment

- Hardware root of trust
  - A basis for system integrity
- Integrity through Trusted Boot
- Secure peripheral access
  - Screen, keypad, fingerprint sensor etc.
- Secure application execution
- Technology called TrustZone®
- Trust established outwards
  - With normal world apps
  - With internet/cloud apps
ARM Trusted Firmware for 64-bit ARMv8-A

The Basics…

- **Standardized EL3 Runtime Firmware**
  - For all 64-bit ARMv8-A systems
- **Reducing porting and integration work**
  - For SoC and Trusted OS developers
- **Reusable, reference implementations**
  - PSCI
  - SMC Calling Convention
  - Configuration of ARM hardware
- **Running on ARMv8-A FVPs and Juno**
  - ... and on partner’s silicon
ARM Trusted Firmware for 64-bit ARMv8-A

- Reference boot flows
  - For 64-bit ARMv8-A systems

- Open Source at GitHub
  - BSD License
  - Contributors welcome

- We just released v1.0
  - Lots of partners using it

Key:
- SCP Execution
- EL3 Execution
- Secure-EL1 Execution
- EL2 Execution

BL3 Non-Trusted Firmware (e.g. U-Boot, EDK2)

BL3 Secure-EL1 Payload
- Trusted OS Kernel

BL31 EL3 Runtime Firmware
- SMCCC
- PSCI
- World Switch Library
- S-EL1 Payload Dispatch

BL30 SCP Runtime Firmware
- System & Power Control

BL0 SCP Boot ROM
- Platform Boot Initialization

BL1 AP Boot ROM
- Trusted Board Boot

Ist level Boot Loader (BL1)
- loads 2nd level image

2nd level Boot Loader (BL2)
- loads all 3rd level images

Application Processor (AP)
Security Profiles

- **Invasive HW Attacks**
  - Well resourced and funded
  - Unlimited time, money & equipment.

- **Non-invasive HW Attacks**
  - Physical access to device – JTAG, Bus Probing, IO Pins, etc.

- **Software Attacks**
  - Malware & Viruses
  - Social engineering

- **SmartCards / HSMs**
4 Compartment Model – Hierarchy of Trust

- **Secure Domain**
  - Secure Element
  - Smartcard
  - SIM & TPM
  - Tamper Proof, Physically Isolated, EAL Certified
  - **SecurCore™ SEE**

- **Trusted Domain**
  - Secure Firmware
  - Device Management
  - Key Management
  - Trusted Applications executing from a Trusted Execution Environment
  - **TrustZone® TEE**

- **Protected Domain**
  - Protected Video Path
  - BYOD
  - System Management
  - Virtual Machines and bus masters isolated by a Hypervisor
  - **Hypervisor HYP**

- **Rich Domain**
  - User Apps
  - Rich OS
  - Android or other OS
  - Privileged Supervisor Mode
Use Cases: Content Protection

TRUSTED MEDIA PROTECTION PLATFORM v1

Processor Cluster (1 to 8 CPUs)

Non-Trusted CPUs

Apps

User RichOS

TRUSTED MEDIA PROTECTION PLATFORM v1

Display

HDMI

VIDEO DECODER

MÄLI V500

AUDIo DECODER

GPU

CRypto

DISPLAY HDMI

NSAID = DISPLAY

NSAID = VIDEO

NSAID = AUDIO

INTERCONNECT

TZASC 400

trusted Boot ROM

trusted SRAM

trusted Peripherals Efuse

DDR

display

video

audio

RICH OS

Engines Firmware

Data Structures

Frame Buffers

FLASH

SoC Firmwares

TEE addition for the TZMPv1 Protection Platform

Non-Trusted World

Trusted World (ARM TrustZone hardware extension)

Protected World (ARM NSAID hardware extension)

*Non-Secure Access ID

ARM®

DRM & Keys protected by TEE Hardware isolated video path
Use Cases: MDM & Enterprise

Samsung Knox

- **APP LEVEL**: SANDBOX
- **KERNEL LEVEL**: KNOX FRAMEWORK
  - SE ANDROID
  - TRUSTZONE™ SYSTEM-ON-CHIP
  - TOUCHSCREEN
  - DEVICE DISPLAY
- **HARDWARE LEVEL**: TRUSTZONE™
- **PERIPHERAL LEVEL**: TRUSTED APPLICATION

**MDM & Enterprise**

- Trusted Boot
- Integrity Management (TIMA)
- MDM
- Business Apps...

- Secure Boot
- Isolated Peripheral Connection
- Trusted Execution Environment (TEE)
  - Hardware Isolation
  - Microkernel Separation
  - Managed Domains for Trusted Applications
  - Privileged Peripheral Access
Use Cases: Payment

Merchant Site
Merchant World

Merchant Shopping
The merchant 'pay now' element drives the TrustZone app to launch, delivering the necessary information to be displayed

Merchant Confirm
A confirmation is returned to the merchant to confirm the payment was successfully taken

Rich OS Normal World

1. Payment Details
Merchant and price of the transaction are confirmed before payment takes place.

2. Secure Handover
Control of user interface is handed over to TrustZone

Authentication & Keys protected by TEE

3. PIN Entry
The PIN is captured through TrustZone hardware and secured by a trusted application before being passed back to the

4. PIN Check & Authorisation
The rich OS regains control, submits the encrypted PIN to the Secure Element for checking, and submits the transaction to merchant payment gateway
Modern Practice

- 3 New whitepapers from Apple, Samsung and Microsoft give good insight into modern mobile security practice

- Build on principles of:
  - H/W roots of trust
  - Trusted Boot
  - Isolation
  - Least Privilege
Agenda

- Introduction
- Four Compartment Security Model
- Emerging Trends
  - Trusted Apps
  - FIDO – Moving beyond passwords
- Summary
TRUSTONIC enables devices with a root-of-trust and Trusted Execution Environment (TEE) at manufacture and sells ACCESS to service providers in need of TRUST.
Connecting Trusted Device Supply with Service Provision

Enriching, simplifying, and expanding people’s digital lives by securing valued services on smart devices.
FIDO User Experiences

PASSWORDLESS EXPERIENCE (UAF standards)

Transaction Detail → Show a biometric → Done

SECOND FACTOR EXPERIENCE (U2F standards)

Login & Password → Insert Dongle, Press button → Done
FIDO UAF* Functionality

- Discovery of authenticators on the client
- Registration
- Authentication
- Transaction Confirmation

*Universal Authentication Framework
How does FIDO UAF work?

FIDO Authenticators

Verification

FIDO SERVER
FIDO - Universal Authentication Framework

User Side

- Plugin
- SDK

- FIDO Client
  - Authenticator Abstraction

- Authenticators
  - Private Keys
    - Authentication Keys
    - Attestation Key

Relying Party

- Web Application
- FIDO UAF Server
  - Attestation Manager
  - Crypto
  - Policy Rules

- Public Keys
  - Authentication Keys
  - Attestation Key

UAF Protocol

Registration, Authentication & Transaction Confirmation

Ideal for TrustZone based TEE
First FIDO Deployment already live…

Customers can use their finger to pay with PayPal from their new Samsung Galaxy S5 because the FIDO Ready™ software on the device securely communicates between the fingerprint sensor on their device and PayPal’s service in the cloud. The only information the device shares with PayPal is a unique cryptographic “public key” that allows PayPal to verify the identity of the customer without having to store any biometric information on PayPal’s servers.
FIDO Implementation Using TrustZone based TEE

- FIDO Client & APIs
- ARM Trusted Firmware
- Crypto Layer
Summary

- FIDO is rapidly building momentum to transform authentication
  - Creates a delightful consumer experience
  - Provides stronger authentication to Relying Parties
  - Well thought out Privacy Principles

- TrustZone based TEE is a perfect fit as an implementation strategy
  - Confidentiality, Integrity and Trusted Peripherals
  - Can be extended to interface to Secure Element if required

- Please study FIDO & TEE!
References

- Samsung Knox™ 2.0 Whitepaper

- iOS Security

- ARM Security Model
  [http://community.arm.com/docs/DOC-8376](http://community.arm.com/docs/DOC-8376)