[pre-show entertainment] ‘Lil Perspective

1956, a 5 MB HDD by IBM

A “smart” phone
Security Adoption Cycle

- Ignore
- Ignore
- Ignore
- Security engineer begs
- Other features
- Exploit's published
- "Oh No"
- "Oh fuck"
- Security

[pre-show entertainment]
An Introduction to TrustZone®, TEE, TLK

Hadi Nahari
Chief Security Architect
NVIDIA

06.04.2013
Trusted Infrastructure Workshop
The Pennsylvania State University, PA
Hadi’s Background

- Trusted & secure computing base, cryptography, complex system analysis, HPC, massively scalable systems design, implementation, and governance

- Identity management, asset protection, information-assurance schemes, vulnerability assessment and threat analysis

- Enterprise & Embedded (Netscape, Sun Microsystems, U.S. gov’t, Motorola, Zaplet, MontaVista, eBay, PayPal, NVIDIA…)

- Co-author of series of GlobalPlatform TEE, NFC and security specifications


- Currently Chief Security Architect at NVIDIA
Blockbuster games consistently outsell the biggest Hollywood films — *Call of Duty: Black Ops 2* reached $500M in sales in its first 24 hours. By 2016, the PC gaming market is expected to reach over $20B. GeForce GPUs are the engines behind the creation and enjoyment of this thriving market.
GPU
GeForce®, Quadro®, Tesla®

Mobile
Tegra®

HPC
VGX™ GRID™
NVIDIA awakened the world to computer graphics when it invented the GPU in 1999. From its roots in visual computing, the company expanded into super, mobile and cloud computing. Today its processors power experiences across the computing spectrum. Founded in 1993, NVIDIA has 8,000 employees and more than 5,000 patents granted or pending.
With a peak performance of 27 petaflops, the Titan supercomputer at Oak Ridge National Labs is the world’s fastest. 18,688 GPUs provide 90% of the machine’s computing power.
Computer graphics commonly enhance live broadcasts using augmented reality. Here, Monday Night Football is enhanced with special effects created using Sportvision’s 1st and Ten Line and Pass Track systems. Graphics generated by Quadro blend in seamlessly with the live video.
Bring Magic to Every Pixel

By 2015, there will be 4B+ HD displays on the planet. Visual computing will increasingly become part of the fabric of society. NVIDIA is singularly focused on the medium that we have propelled from a feature into an industry. We aim to light every pixel.

Source: DisplaySearch
Agenda

- Trust & Security
- TrustZone® & HW-TCB
- TEE & GlobalPlatform
- TLK: a FOSS stack
- Conclusion, Q&A
Agenda

- Trust & Security
- TrustZone® & HW-TCB
- TEE & GlobalPlatform
- TLK: a FOSS stack
- Conclusion, Q&A
Trust & Security

- TCB requires agreement on Trust Boundary
- Trust is a contract; an agreement
- Trust !≠ Security
- Security is a verifiable assertion
  - Subset of QA
  - Trust but verify
- Security is meaningless without
  - Assets
  - Attacks
- Security to system is harmony to music

The Information-Centric Security Lifecycle

- Create: Classify, Assign Rights
- Store: Access Controls, Encryption, Rights Management, Content Discovery
- Use: Activity Monitoring, and Enforcement, Rights Management, Logical Controls, Application Security
- Share: CMP (OIDP), Encryption, Asset Management
- Archive: Encryption, Asset Management
- Destroy: Crypto-Shredding, Secure Deletion, Content Discovery
Computing Trends
Security Trends
Observations

- Service-end security ➔ northbound
- Device-end security ➔ southbound
- Security usability (hence adoption) ➔ unacceptable in either and
- [Almost] no holistic, E2E security ➔ consumer loses
Agenda

- Trust & Security
- TrustZone® & HW-TCB
- TEE & GlobalPlatform
- TLK: a FOSS stack
- Conclusion, Q&A
TrustZone®

Normal world
- Normal world user mode
- Normal world privileged modes

Secure world
- Secure world user mode
- Secure world privileged modes

Monitor mode
TrustZone® and Hardware-based TCB

- Each of the physical processor cores provide two virtual cores
  - Secure (Secure World for the security subsystem)
  - Non-secure (Normal World for everything else)

- New core mode: Monitor Mode
  - A mechanism to context-switch between two states (secure ⇔ non-secure)

- A limited set of mechanisms to enter the Monitor Mode
  - S/W: SMC instruction from software
  - H/W: IRQ, FIQ, external (prefetch, Data) aborts
The NS bit in the SCR in CP15 indicates which state (aka “world”) the processor is currently in:

- NS = 1 ➞ processor is in non-secure state
- NS = 0 ➞ processor is in secure state
- SCR can only be accessed in secure state

Monitor Mode is always running in secure state regardless of the value of NS bit.
TrustZone® Secure Interrupts

ARM recommendation:
- IRQ for normal world
- FIQ for secure world

IRQ and FIQ can be directly trapped to Monitor Mode

Vector Based Address Register
- For non-secure, secure, and monitor
Agenda

- Trust & Security
- TrustZone® & HW-TCB
- TEE & GlobalPlatform
- TLK: a FOSS stack
- Conclusion, Q&A
TEE: Trusted Execution Environment

- A carve-out within Application Processor (AP)
  - Allows for running a trusted piece of code
  - Provides hardware-based isolation
  - Enables privileged access to device resources (e.g. memory, hardware crypto accelerator(s), etc.)

- ARM TrustZone is one way to implement a TEE
GlobalPlatform™ and TEE

- TEE WG of GlobalPlatform™ standardizes the TEE & its APIs

GlobalPlatform™*

- GlobalPlatform works across industries to identify, develop and publish specifications which facilitate the secure and interoperable deployment and management of multiple embedded applications on secure chip technology. **GlobalPlatform Specifications** enable trusted end-to-end solutions which serve multiple actors and support several business models.

  (source: [http://www.globalplatform.org/aboutusmission.asp](http://www.globalplatform.org/aboutusmission.asp))
Main TEE ecosystem roles/entities
- Chip vendor
- Device vendor (OEM/ODM)
- TEE stack vendor
- TSM (Trusted Service Manager)
- SP (Service Provider)
- TA (Trusted Application) provider

Each entity has a specific role: defined by GlobalPlatform™
TEE stack vendors usually play TSM role as well
TEE Use Cases

- Mobile payment
- Runtime integrity verification
- Trusted user interface
- Remote enablement/disablement
- Automotive (trust vs. safety)
- Secure isolation, Remote attestation
- DRM, HDCP, secure NFC in P2P mode
- Any other operation that requires verifiable trust
Example: Mobile Payment Per GP

- Application Developer
- SIM Manufacturer
- Acquirer
- Merchant
- Consumer
- Phone Manufacturer
- Internet
- Settlement
- Issuer
- Mobile Network Operators
- Trusted Services Manager

Legend:
- Pink: Mobile Fraud Risk: new environments & entities
- Yellow: Financial Fraud Risk: legacy environments & entities
- Blue: Legacy payments relationships
Agenda

- Trust & Security
- TrustZone® & HW-TCB
- TEE & GlobalPlatform
- TLK: a FOSS stack
- Conclusion, Q&A
**TLK: Trusted Little Kernel**

**What**
- An open source and royalty free software (i.e. FOSS) stack for TrustZone® to accelerate the adoption of hardware-based security for SoC, device, system, and service providers

**Why**
- Kerckhoffs’s Desiderata
- As of ARMv6KZ *almost* all ARM-based devices ship with the necessary hardware
  - ~1.7M Android devices enabled each day
- Enabling a more secure ecosystem
- Existing TrustZone® software stacks might face challenges supporting all requirements of Defense & Intelligence Communities
TLK’s base

TLK is based on LK (Little Kernel)

LK

- ~63000 LOC in C, with ARM emulation .bin ~22KB
- Small, pre-emptive kernel
- Supports Cortex-M3, Cortex-A8, AVR32, x86 SoC families
- Supports multi-threading, IPCs, and thread scheduling
- No TrustZone® features present
- MIT/FreeBSD license
- Designed, implemented and maintained by Travis Geiselbrecht, et al
TLK General Design Criteria

- Open source
- Interrupt & SMP
- Open tools (e.g. gcc)
- Secure timer
- Deferred startup of services
- crypto ops

- Extensible
- Code
  - Clean
  - Small size
  - Well structured
- Easy to learn
- Existing security constructs
TLK Features

- Cortex A9 & A15 support ➔ complete
- LP2 (on slave CPU) ➔ complete
- SMC handler ➔ complete
- Boot to Normal World ➔ complete
- Page table management ➔ complete
- Addition of user mode ➔ complete
- 2 MB carve-out ➔ complete
- Addition of syscalls ➔ complete
- Addition of libc ➔ complete
- Address-space separation ➔ complete
TLK Features (cont’d)

- Task configuration (stack/heap size, UUID) from manifest ➔ complete
- Multiple task loaded/runnable (called out by UUID) ➔ complete
- Task execution (linker script aligning TA text/data) ➔ complete
- NEON support (lazy context switching between NS apps and tasks in Secure World) ➔ complete
- Buffer handling between worlds, as well as TAs (by reference; explicit syncing required) ➔ complete
TLK Features (cont’d)

- Issue task-to-task requests ➔ **complete**
- CryptoLib based on OpenSSL ➔ **complete**
- Tasks requesting mappings to HW ➔ **complete**
- Discovery and set-up of HW in Normal World-usable state, setting up the SCU (to maintain data cache coherency), GIC, CP15 state of SMP, ARM errata (for boot & slave CPUs post-reset) ➔ **complete**
TLK Features (cont’d)

- L1, L2 clean/inval/flush over a range ➔ complete
- Securing TLK carve out ➔ complete
- LP2 ➔ complete, LP1 ➔ complete
- Crypto drivers (crypto ops, key handling) ➔ complete
- Power management (selective L2 flush, CPU suspnd-rsme, driver suspnd-rsme) ➔ complete
- Static task loading (services/drivers) ➔ complete
- HW sharing with the NS world ➔ underway
- Secure timers ➔ underway
TLK Stats

- **tlk.bin**
  - Memory carve-out: 2MB
  - With thread context switch, task bootloader, 5 services and usermode TAs (including full WV) and libc/libtsksvc and all the required kernel support: **477KB** (debug and logging enabled)

- **Less than 5% Tegra-specific code**
Thank You

Q&A

Hadi Nahari
hnahari@nvidia.com
hadinahari
www.linkedin.com/in/hadinahari

Rates chart
✴ Answers: $1
✴ Correct answers: $3
✴ Correct answers (requiring thought): $5
✴ (dumb looks still free)