Bringing Android to Secure SDRs

David Kleidermacher

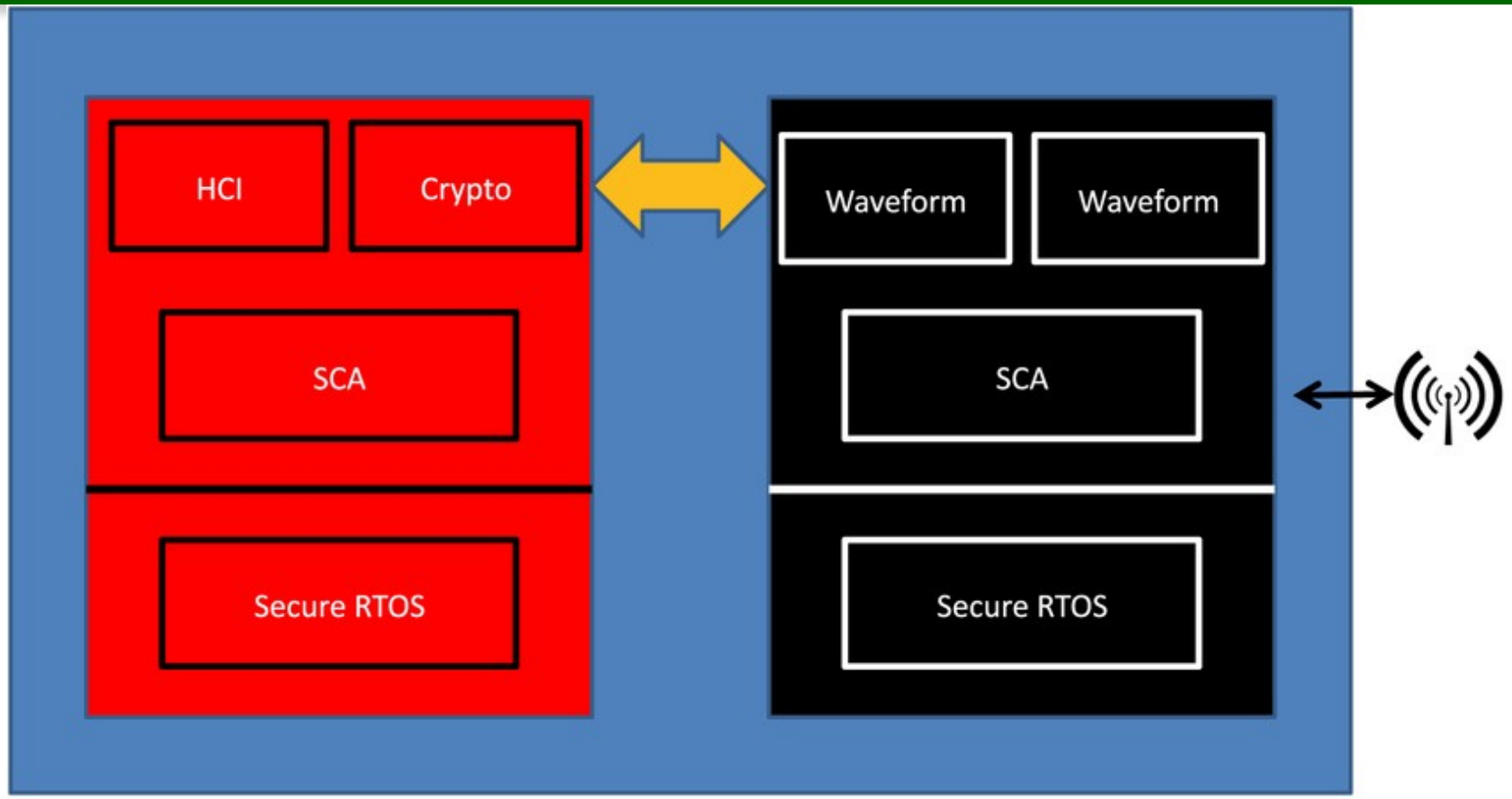
Frank Vandenberg

SDR'11 – WinnComm - Europe

Agenda

- Overview – Why Android in SDR?
- Android Security
- Proposed Architecture

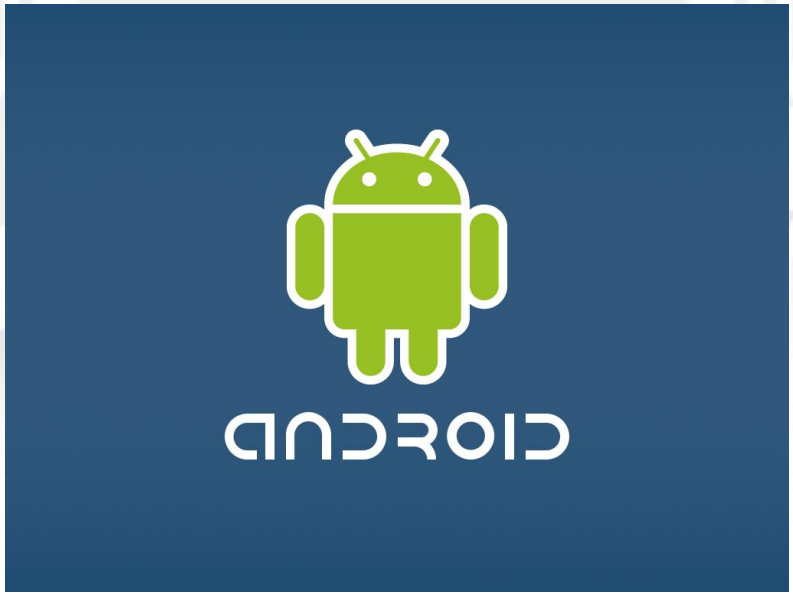
Typical red-black architecture for military SDR



HCI is mission-critical and must be trusted and certified; therefore often custom
Note: Crypto usually on separate discrete but logically “red”

Why Android in SDR?

- More sophisticated HCIs are desired
  - Powerful GUI for control and management
- Stay current on technology – avoid expensive custom interfaces
- Open source licensing
- Powerful apps environment



Android Security Today

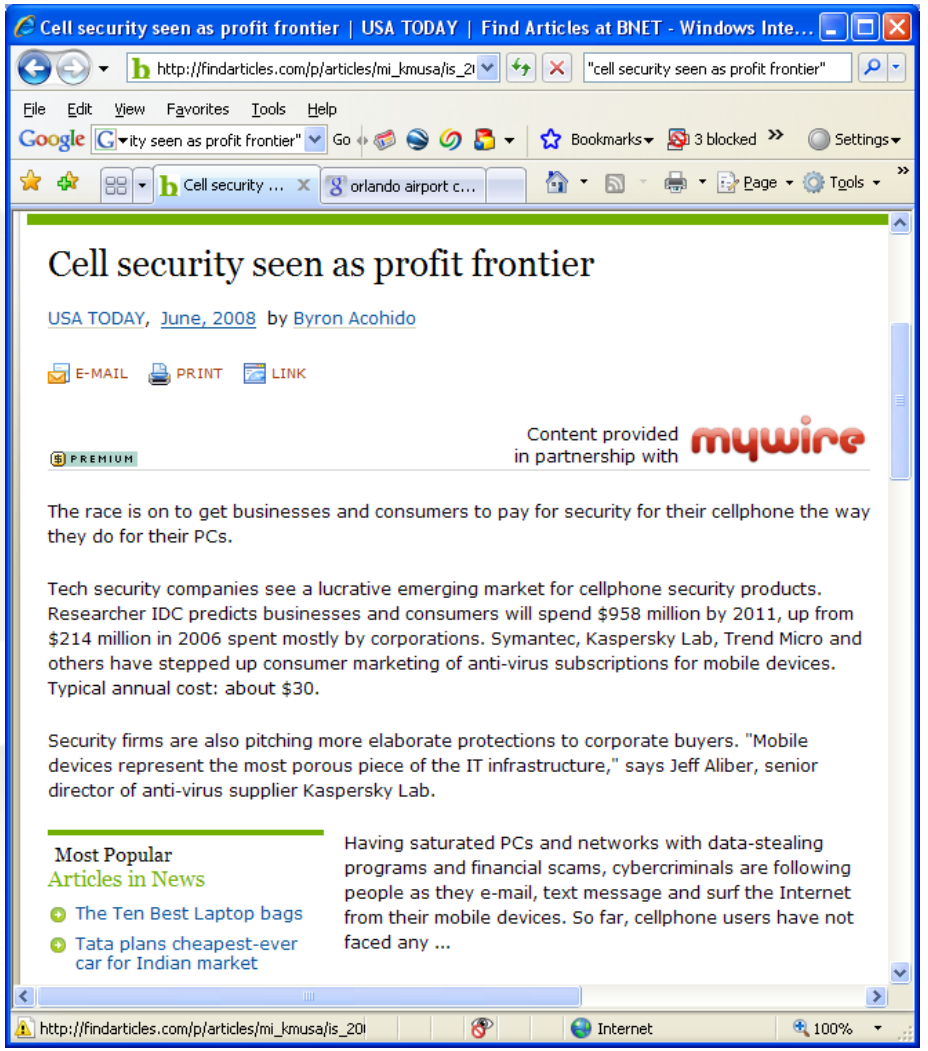
- Google Android – G1 released September 22, 2008
  - Oct. 24: NY times reports serious browser vulnerability – from open-source
  - Nov. 6: “Just this week, however, hackers discovered a way to install applications natively on the phone.” ZDNet: “Worst. Bug. Ever.”
  - Nov. 11: "We tried really hard to secure Android. This is definitely a big bug. The reason why we consider it a large security issue is because root access on the device breaks our application sandbox."
- Lots more since...
  - CVE-2009-2999, -2656: allows remote attackers to cause a denial of service (application restart and network disconnection)
  - CVE-2009-1754: allows remote attackers to access application data
  - CVE-2009-0608, -0607: buffer overflows with unknown impact
  - CVE-2009-0985, -0986: buffer overflows allow remote attackers to execute arbitrary code

Android Security Today

- Android is built on Linux
  - Explosive growth in complexity over time
  - 20,000 LOC changed per day
  - Kernel grew from 5 to 11 Million LOC in 2.6 era
  - CVE-2009-2692 - “The Proto-Ops Vulnerability”
    - Trivial user-mode app can take over the system
    - Latent in Linux kernel for 8 years

Android Security Today

- "Mobile devices represent the most porous piece of the IT infrastructure"
- "Like the early days of Web applications, people throwing code together as fast as they can, giving no thought to security"
- "The more sensitive data you store on that device, the more valuable it is to an attacker"



What is Secure?

- Common Criteria Security Levels: 1-7
  - EAL 4: Windows, Linux, VMware
    - “protection against …inadvertent or casual attempts to breach the system security”
    - not for protection “against determined attempts by hostile and well funded attackers to breach system security.”
- EAL 6+ / High Robustness
  - Government program to protect secrets
    - The most valuable resources exposed to the most sophisticated attackers
    - Formal methods, NSA pen testing


National Information Assurance Partnership

Common Criteria Certificate

Common Criteria

is awarded to

Green Hills Software, Inc.

Note: This evaluation contains results that are not mutually recognized in accordance with the provisions of the CCRA; only the evaluation results of EAL4 components are mutually recognized.

The IT product identified in this certificate has been evaluated at an accredited testing laboratory using the Common Methodology for IT Security Evaluation (Version 2.3) for conformance to the Common Criteria for IT Security Evaluation (Version 2.3) ISO/IEC 15408. This certificate applies only to the specific version and release of the product in its evaluated configuration. The product's functional and assurance security specifications are contained in its security target. The evaluation has been conducted in accordance with the provisions of the NIAP Common Criteria Evaluation and Validation Scheme and the conclusions of the testing laboratory in the evaluation technical report are consistent with the evidence adduced. This certificate is not an endorsement of the IT product by any agency of the U.S. Government and no warranty of the IT product is either expressed or implied.

Product Name: INTEGRITY-178B Separation Kernel
Evaluation Platform: INTEGRITY-178B Real Time Operating System (RTOS), version IN-ICR750-0101-GH01_Rel running on Compact PCI card, version CPN 944-2021-021 w/PowerPC, version 750CXe
Assurance Level: EAL6+, High Robustness

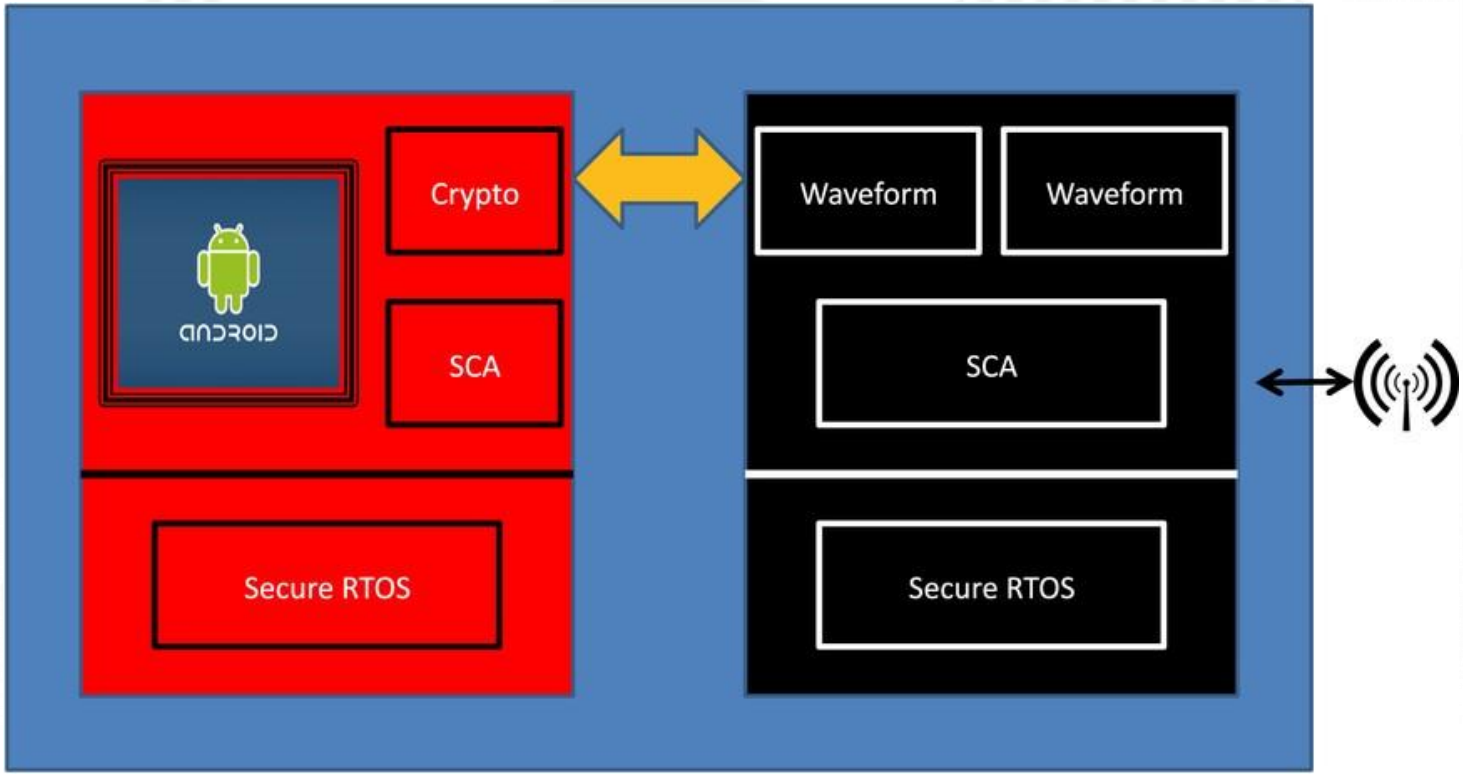
CCTL: Science Applications International Corporation
Validation Report Number: CCEVS-VR-VID10119-2008
Date Issued: 01 September 2008
Protection Profile: US Government Protection Profile for Separation Kernels in Environments Requiring High Robustness, Version 1.03, 29 June 2007

Original Signed By
Director, Common Criteria Evaluation and Validation Scheme
National Information Assurance Partnership

Original Signed By
Information Assurance Director
National Security Agency

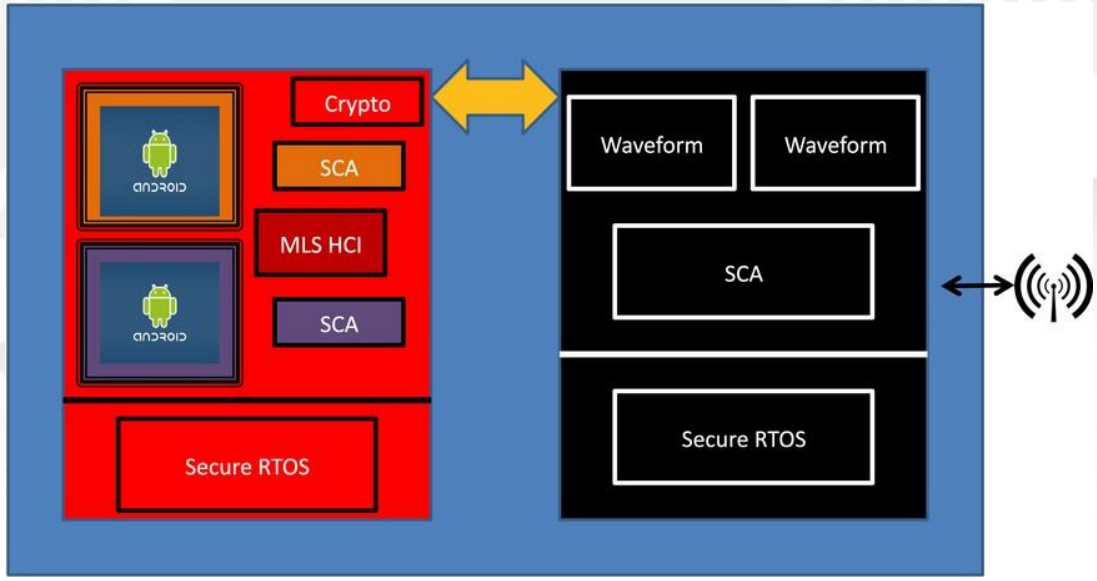
So how do we get Android *and* Security?

- Secondary red-side processor
  - Extra SWaP-C
- Better: MILS Virtualization



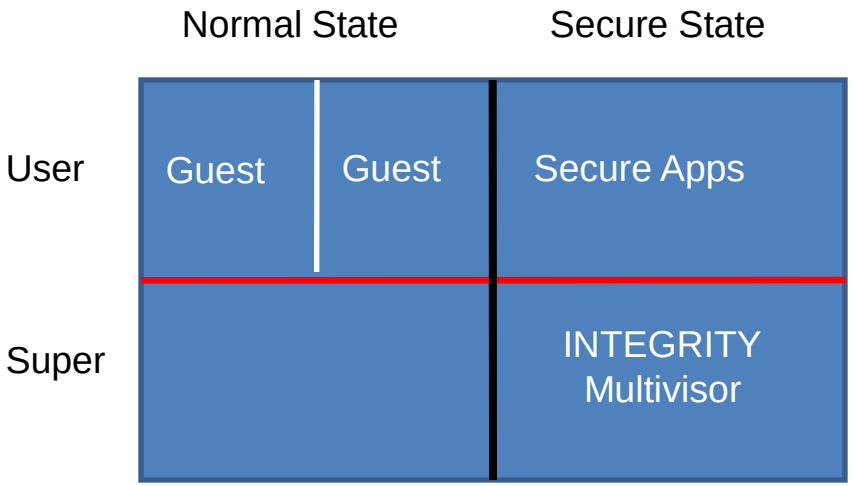
Multi-domain Android

- e.g. Classified and Unclassified in same radio
- Secondary red-side processor
  - Extra SWaP-C
- Better: MILS Virtualization, with a small amount of MLS
- For secret and below, sensitive-but-unclassified, civil/commercial
  - Can do all of this on one SoC (no red-black)



Is this practical?

- Yes!
  - Intel VT
  - Power.org Embedded Virtualization (Freescale QorIQ)
  - ARM TrustZone and VE
- Most JTRS SDRs already using MILS virtualization
  - INTEGRITY Multivisor with virtualized Linux



Summary

- Challenges and Opportunities for SDR
  - Security and real-time required
  - Want powerful Android HCI
    - Android security is poor
- MILS Virtualization provides the ideal combination
  - Trustworthy OS for
    - SCA
    - Secure boot and crypto management
    - Device authentication
    - Secure device drivers
  - The latest and greatest Android
  - Practical on today's modern SDR microprocessors – ARM, Power, Intel

Thank You!