Securing a Commercial off the Shelf (COTS) Smartphone using DoD Technology

To: Systems and Software Technology Conference, April 24, 2012

Information Assurance Products
Richard Takahashi, Director
ITT - Exelis

Objectives

- A secure smartphone using COTS products and DoD technology
  - COTS mode: Preserve smartphone features
  - Secure mode and return safely to COTS mode
- A secure smartphone to leverage commercial products and infrastructures
- Designed for DoD and Federal users based on DoD security requirements
  - Secret and Below voice and data usages
  - Future international-export usages
- Agnostic to the platform and network

Objectives-Continued

- Portable to future platforms with minor modifications
    - Fast port to new smartphone platforms in week/months
- Today the main focus is Android OS v. 4.x based smartphone and tablets
- The solution requires end to end network architecture
- Design based industry open standards from OS to network protocols

Why Android OS?

- Android based products has over 50% market share in 2012 & growing
    - Smartphones and tablets
- Google has open developer platform: Galaxy Nexus (2)
    - Open Source OS
    - Huge world wide developer's group/blogs
- Apple, Window Mobile, RIM, Nokia OS's
    - Proprietary shared-source OS

Challenges

- Android is a general purpose flexible, open OS
- Does open source software development process increases software security or is it detrimental to security?
    - **Currently** Debatable (Development in a Vacuum vs. an Open Forum)
- Current Android OS Security is at risk:
    - Discretionary Access Control (DAC) (based on user & group)
    - No Security Policy - Mandatory Access Control (MAC)
    - The vold - Android volume daemon (mounting as root)
    - No message verification
    - Zygote - Android app spawner (privilege escalation)

Challenges-Continued

- Google has aggressive version releases
  - Since 2007, 4 fours version released, latest is v. 4.x (ice cream sandwich)
- Smartphone vendors has custom features per product lines
- Smartphones have many processors from multiple vendors:
  - Qualcomm, Texas Instruments, Broadcom, NVIDIA, Intel, Custom versions
- And finally...
- Detect and prevent attacks
- Example are malicious malware to covertly snoop and extract crypto information

Three Basic Secure Smartphone Approaches

- All custom hardware and SW design
  - Ground up design
- All SW solution with multi layer SW architecture
  - Use COTS smartphone
- Hybrid using SW and Hardware
  - Use COTS smartphone with software and DoD type technology

Custom Hardware and SW Design

- Advantages
  - Optimum design tightly couples hardware to software OS
  - Custom features not available on COTS
- Disadvantages
  - Very long development time 3-5yrs
  - Obsolete by production time
  - Very limited SW applications
  - Next generation product in 3-5 years

All SW Solution Design

- Advantages
  - Uses a COTS smartphone
  - SW solution is portable (in theory)
  - Use isolation technology: Hypervisor 1 or 2
  - Layering different security protocols are acceptable
- Disadvantages
  - Open OS has thousands + access and testability ports
  - Challenges to prevent & detect malicious modifications
  - End to end system required
  - Challenges to tamper & zeroization

Hybrid HDW (DoD Crypto) & SW Design

- Advantages
  - Uses a COTS smartphone
  - HDW and SW solution is portable (in theory)
  - Use SW isolation technology: Hypervisor 1 or 2
  - Critical crypto functions are protected in isolated trusted hardware
  - Layering different security protocol is acceptable
  - Tamper & zeroization
- Disadvantages
  - Initial hardware crypto module development
  - Still has SW vulnerabilities
  - Challenges to prevent & detect malicious modifications

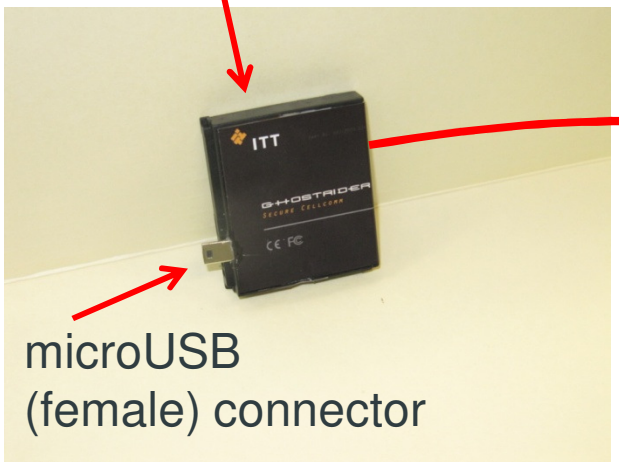
Hybrid HDW (DoD Crypto) & SW Design

- Two types of isolation technologies
- Trusted DoD hardware module to execute critical crypto functions
    - Key management, generation & protection
    - Data at Rest
    - Cross domain protection
    - Tamper & zeroization
- Software: Hypervisor and Virtual Machine
    - A secure isolated OS
    - Protect security applications and direct hardware access
    - Sanitize the phone‘s memories prior to exiting back to the phone’s host Android OS

Hybrid Secure Smartphone
(COTS back cover with integrated Battery/DoD crypto module)

DoD type Crypto Module
Quick Swap without cables
to connect

(DoD Crypto Module with
Battery and integrated DoD
type processor



Hybrid Secure Smartphone
with COTS Back Shell

Hybrid SW Isolation

- The Type-1 (Bare-Metal) embedded Hypervisor will run a micro kernel in an isolation layer tightly coupled to phone's CPU hardware
    - Tightly to the smartphone's CPU processor and hardware
    - Extensive engineering to port
- The Type-2 (Hosted) Hypervisor will run in the kernel and user space of the existing Android OS
    - Android OS runs in a sandbox environment
    - Portable & more easily installed on variety of platforms

Hybrid HDW/SW Isolation

- Isolated crypto function in hardware
  - Benefit: significantly off-load the CPU
- Isolate hardware interfaces using Hypervisor technology
  - Hypervisor Type 1 or Type 2 (preferred)
- Isolate Virtual Machine Image (OS) from hosting hardware
  - HDW can store (encrypted) Secure Android OS image
- Isolate (user and application) access in Secure OS

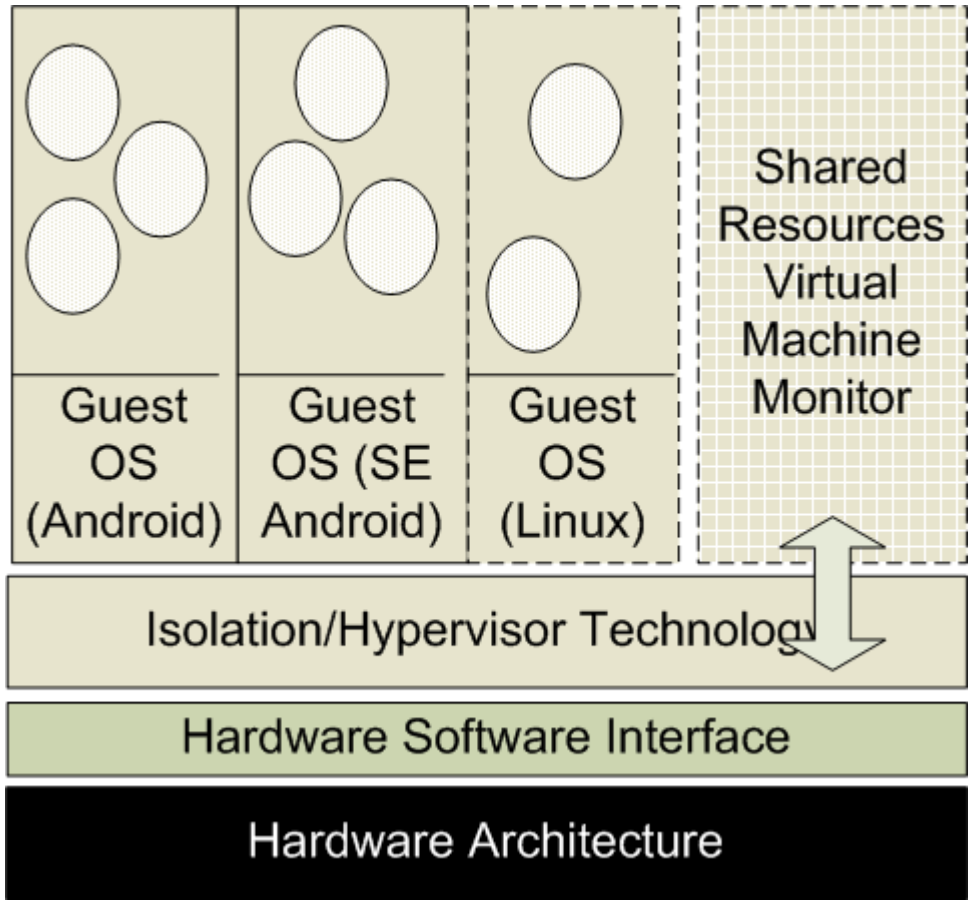
Hybrid HDW/SW Isolation

- SD Card vs. USB Interface (preferred)
  - USB provides high speed host to device communication
    - One to one communication with trusted channel
  - SD Card using SDIO and SD interface (block-addressable storage)
    - Shared mount point between multiple personalities (OS)
    - Additional (Hypervisor) code needed to prevent shared access

Hypervisor Type 1 vs. Type 2

- Hypervisor provides:
  - Multiple, distinct, isolated security domains are now possible on a single Android smartphone
  - Each with their own capabilities, files, encryption, networks, etc.
- Type 1 Hypervisor requires extensive engineering to port
  - Not a timely portable option because of “bare metal” need
  - Provide best protection
- Type 2 Hypervisor is portable but not as secure as Type 1
  - Locking a Type 2 Hypervisor to a trust anchor provide additional protection
- Given time to market and protection is the driver…
  - Hypervisor-type 2 for ease of portability
  - USB based crypto module
  - Locking the Hypervisor-2 to a USB crypto module (trust anchor)

Hypervisor Type 1: Virtualization Block Diagram



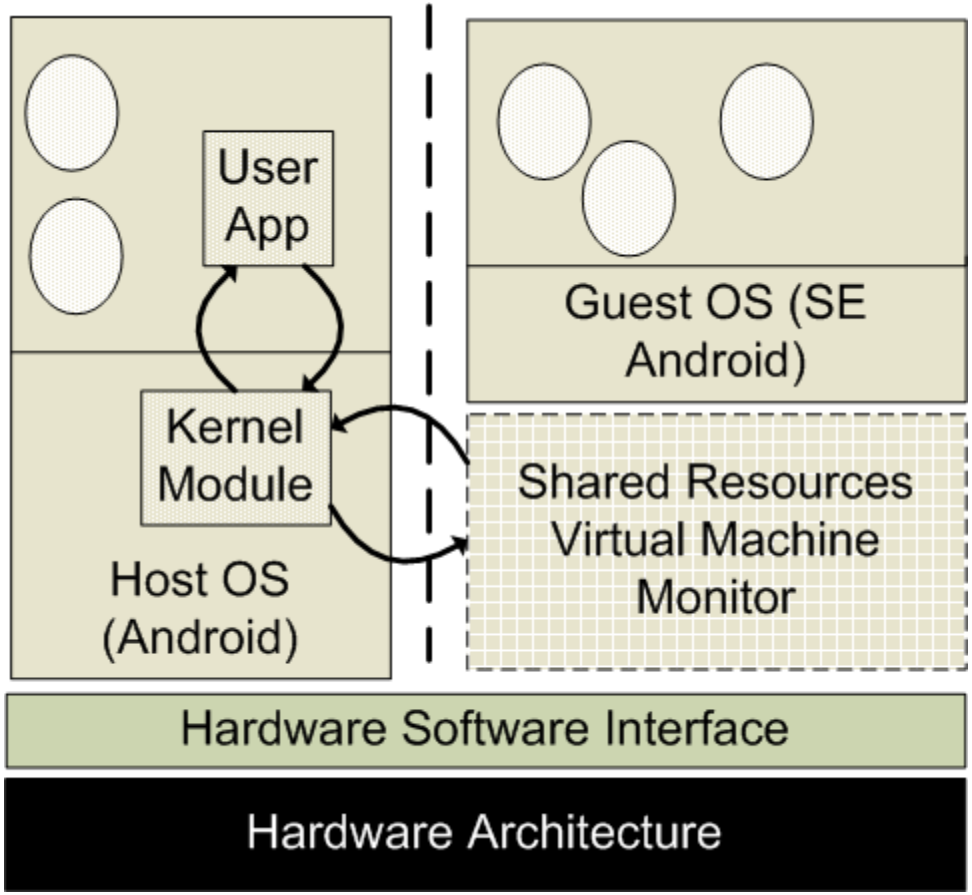
Advantages

- Strong isolation between OS, Apps and drivers
- Tied to CPU - use of ARM-VE or Intel VT
- Smaller trusted computing base

Disadvantages

- Intense engineering effort to port
- Requires tight hardware coupling
- Specific apps and drivers to defend against specific threats
- Processors changing fast
- High performance degradation

Hypervisor Type 2: Virtualization Block Diagram



Advantages

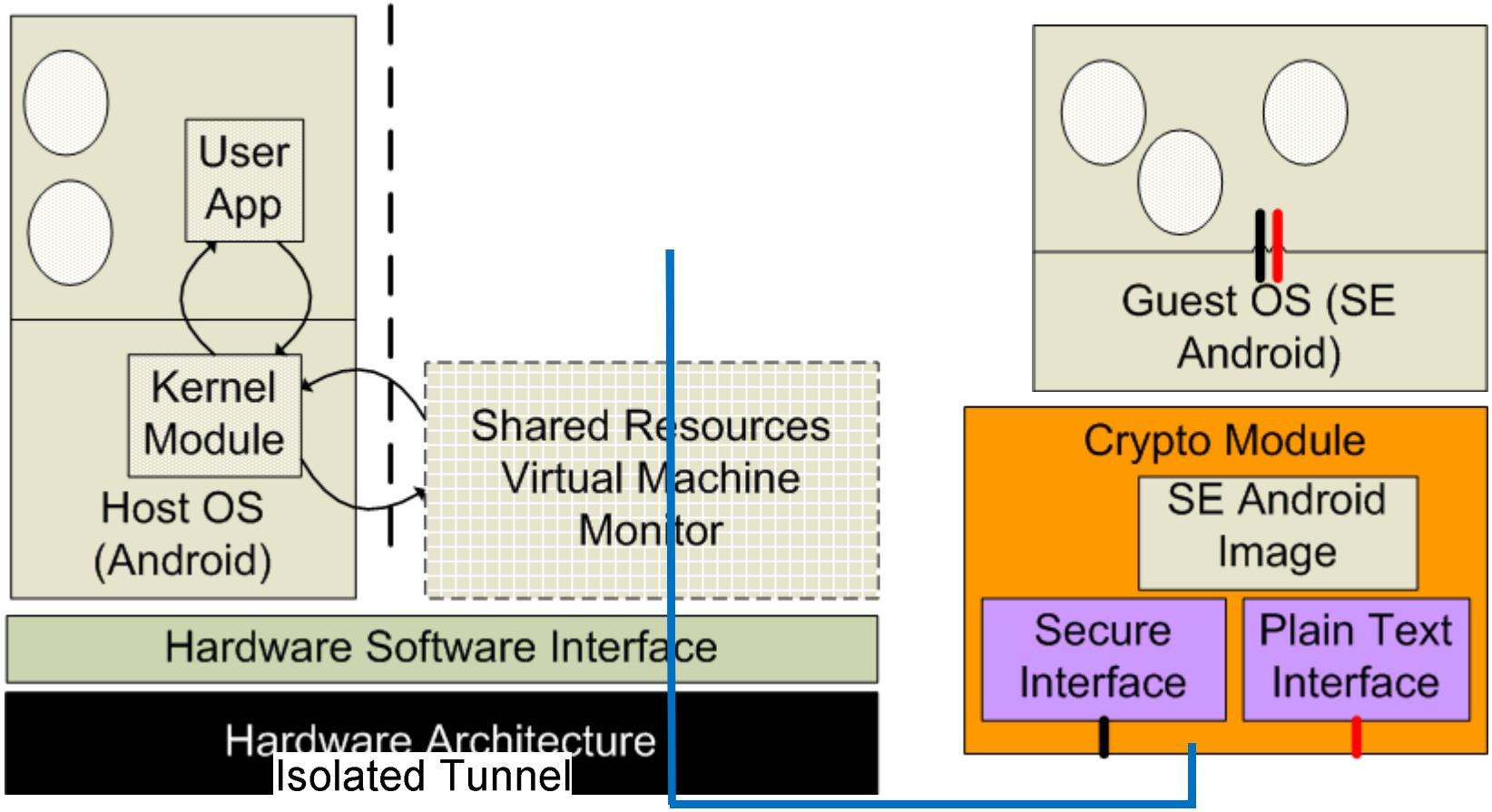
- Portable not tied to hardware
- SW based separation and isolation
- Can run multiple operating systems besides Android (e.g. SE Android, or Windows Mobile etc.)
- Ideal for future upgrades for multiple configurations

Disadvantages

- Security posture depends on host OS
- OSs are SW separated
- Medium performance degradation

Hybrid Isolation Architecture

- Guest OS is downloaded from crypto module
- Crypto module authenticates OS
- Isolated tunnel established



Multi-Personality

- Paravirtualization techniques to support high performance virtual machines
    - Allows for BYOD Solution
- Hypervisor technology allows for multi-personality on a single handset
    - Host OS is the primary operating environment.
    - Each subsequent OS (guest) in the virtual environment may have a different personality
        - Secure Communication
        - Enterprise controlled images

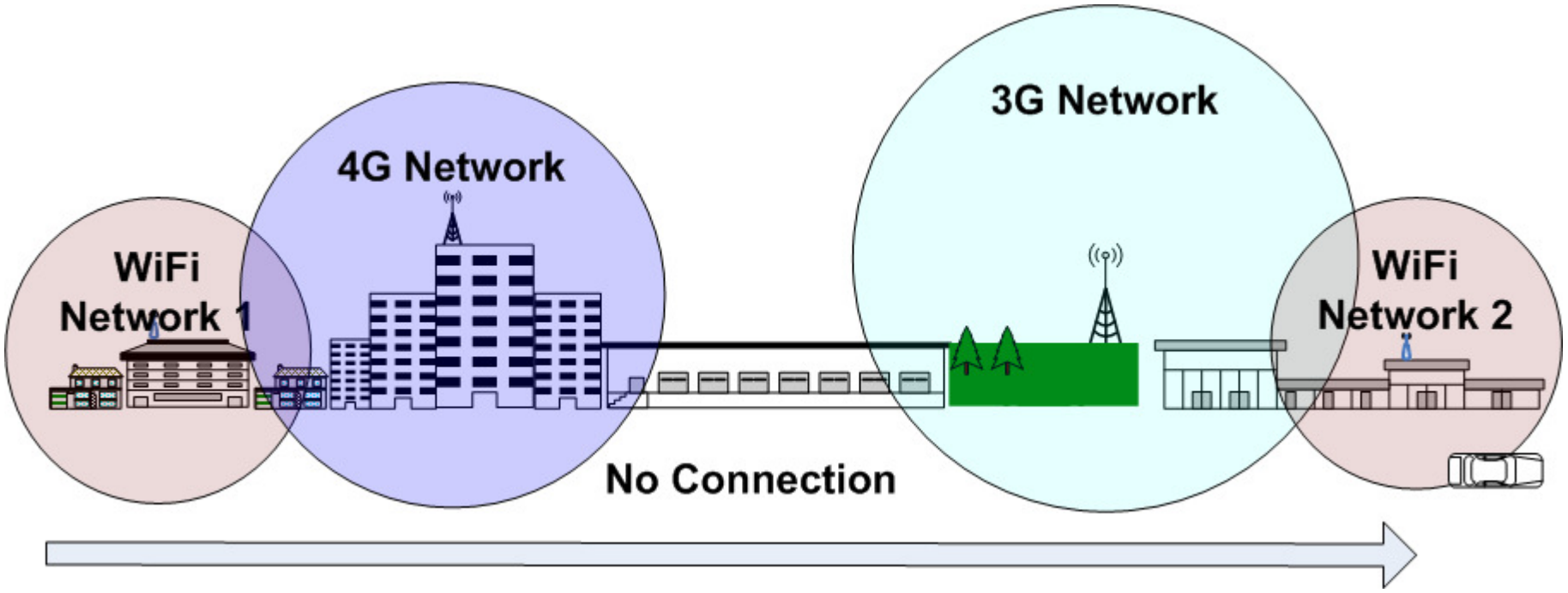
Secure Data in Transit

- Use mobility technologies
  - IKEv2 Mobility and Multihoming Working Group (MOBIKE)
  - Wireless Transport Layer Security Specification (WTLS)

- Layered security for Data in Transit
  - Virtual Private Network (VPN) for host to gateway
    - Mobile VPN (mVPN) - IPSec using IKEv2 with MOBIKE
    - WAP WTLS using secure session based VPN
  - DTLS & DTLS-SRTP for peer to peer communication
  - TLS (HTTPS) for client to server communication

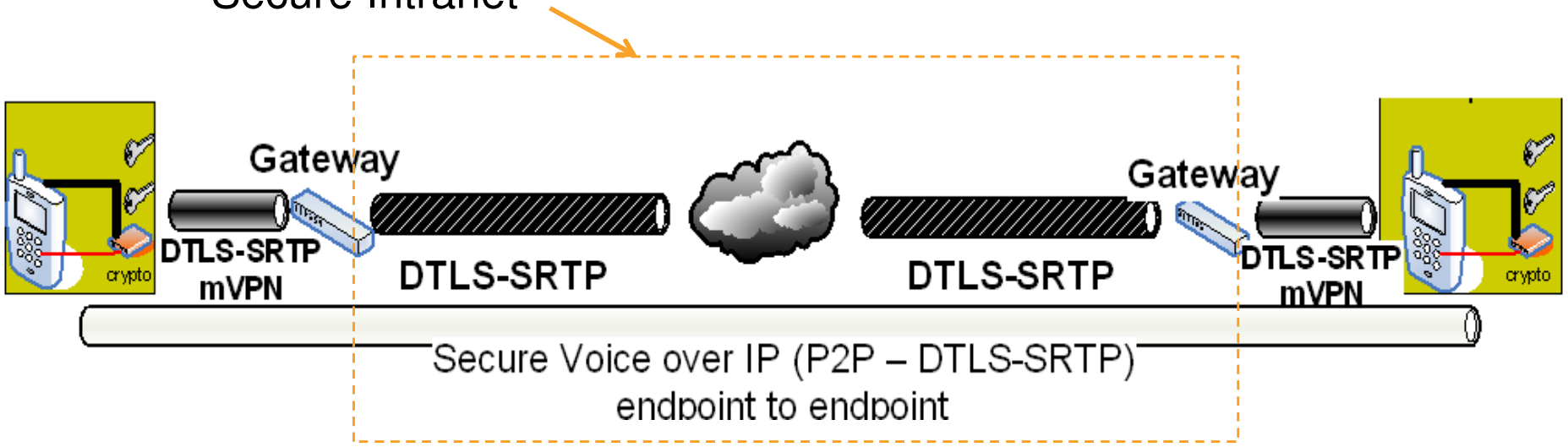
Secure Data in Transit

- Challenges with IP Addresses
  - NAT, proxy, wireless technologies (WiFi, CDMA, GSM, UMTS, LTE)
- Current cellular network were not designed for continuous data usage
  - Service providers are controlling by throttling, controlling data rate



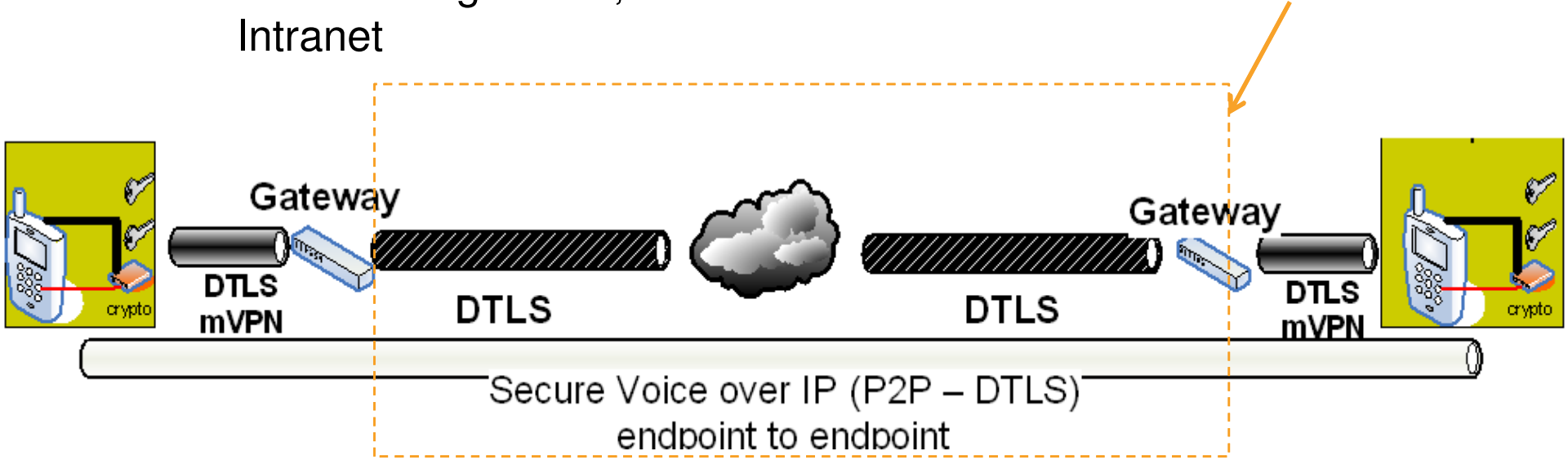
Voice (VoIP) Communication Mode

- DTLS-SRTP will be used to handle the security for peer to peer voice communication
  - A secure peer-to-peer link will be created between smartphones allowing for SRTP communication
  - Secure mobile VPN using IPSec (or WTLS) between smartphones and gateway
  - In this configuration, the SIP and Relay server will reside in the Secure Intranet



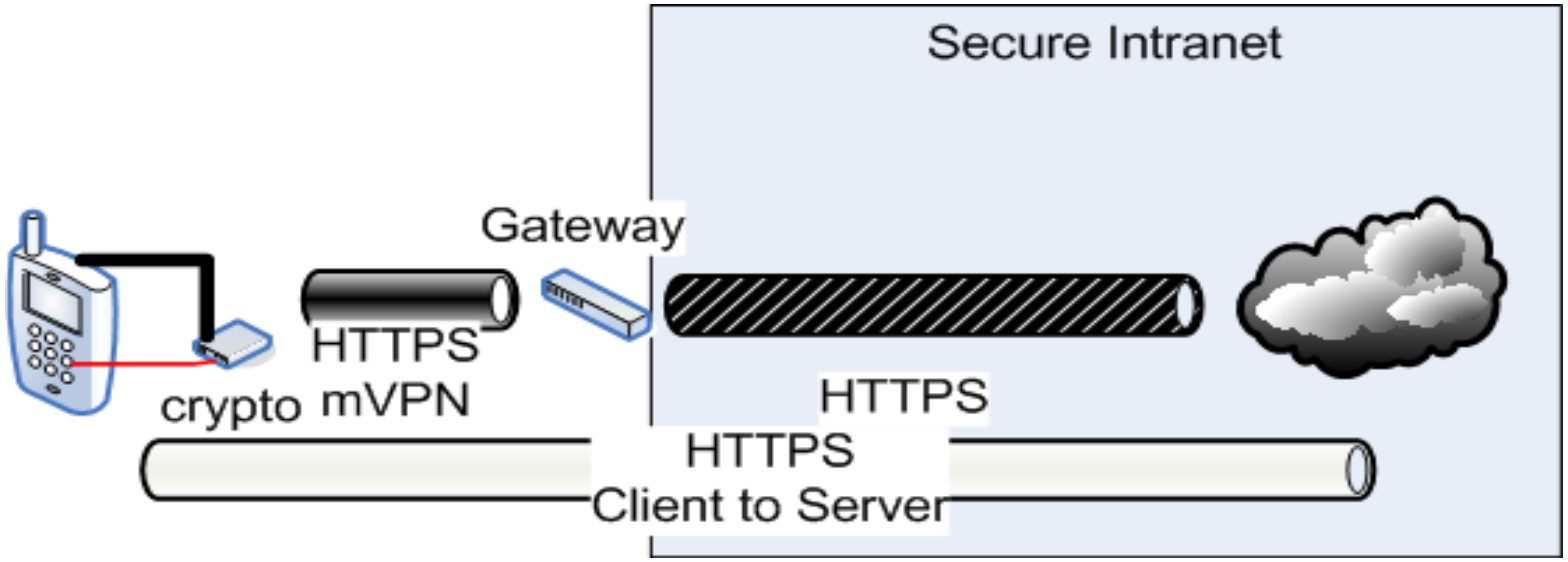
Data (IMS-Text) Communication Mode

- DTLS maybe used to handle the security for peer to peer data (text) communication
  - A secure peer-to-peer link will be created between secure smartphones allowing for DTLS based communication
  - Secure mobile VPN using IPSec (or WTLS) between secure smartphones and gateway
  - In this configuration, the IMS server will reside in the Secure Intranet



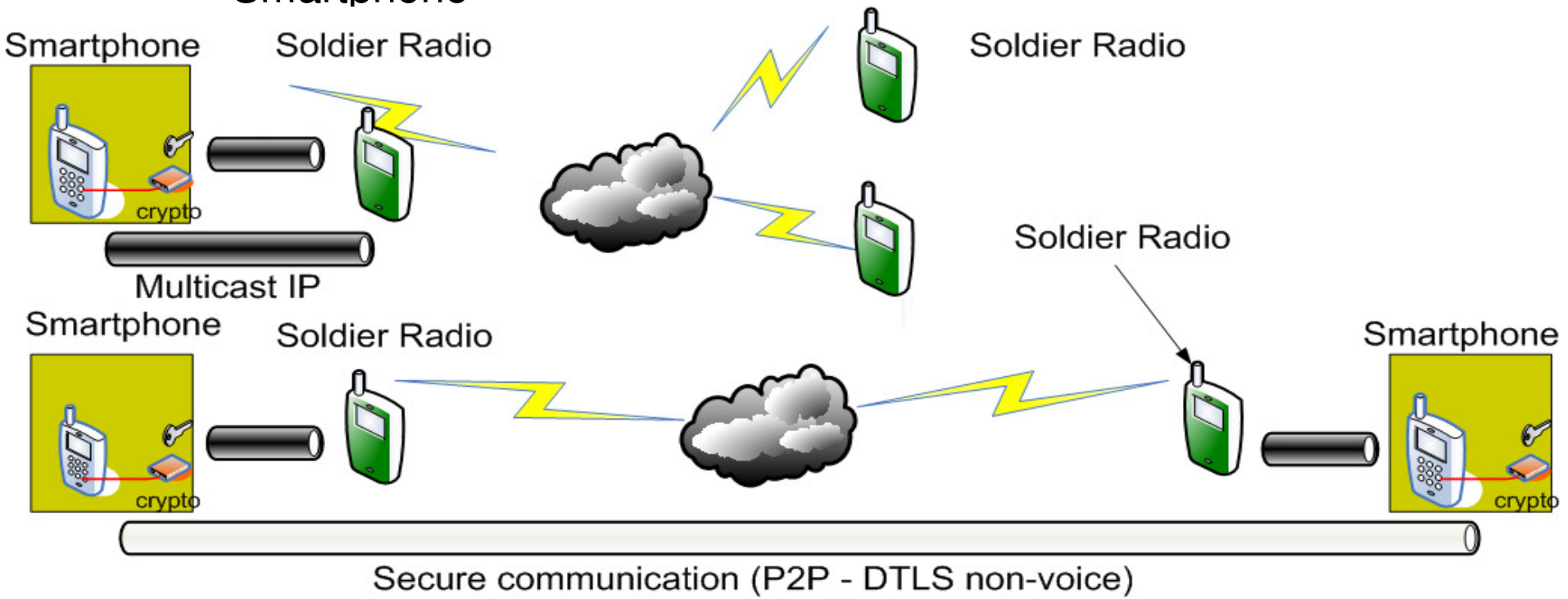
Data Communication Mode

- HTTPS maybe used to handle the security for client server data communication
  - A secure client-server link will be created between secure smartphone allowing for secure communication
  - Secure mobile VPN using IPSec (or WTLS) between secure smartphones and gateway
  - In this configuration, the server will reside in the Secure Intranet



Cross Domain Mode

- In Cross Domain (data diode) mode, data from a Soldier Radio will be passed through to smartphone to the Situational Awareness application
  - IP data from smartphone will be encrypted by the crypto module
  - Soldier Radio uses multicast addressing to route data to the Secure Smartphone



Questions?

Thank You!

Acronyms

API	Application Programmers Interface
ARM	Advanced RISC Machine
ARM-VE	ARM Virtual Extension
ASIC	Application Specific Integrated Circuit
BYOD	Bring Your Own Device
CDMA	Code division multiple access
COTS	Commercial Off the Shelf
CPU	Central Processing Unit
DAC	Discretionary Access Control
DAC	Discretionary Access Control
DoD	Department of Defense
DTLS	Datagram Transport Layer Security
FPGA	Field Programmable Gate Array
GSM	Global System for Mobile Communications
HDW	Hardware
HTTPS	Hypertext Transfer Protocol Secure
IMS	IP Multimedia Subsystem
Intel VT	Intel Virtualization Technology
IP	Internet Protocol
IPSec	Internet Protocol Security
KMI	Key Management Initiative

LTE	3GPP Long Term Evolution
MAC	Mandatory Access Control
MOBIKE	IKEv2 Mobility and Multihoming Working Group
OS	Operating System
PLI	Program Language Interface
RISC	Reduced Instruction Set Computer
SAB	Secret And Below
SDIO	SDIO (Secure Digital Input Output) card
SD	Secure Digital
SE Android	Security Enhanced Android OS
SIP	Secure Internet Protocol
SRTP	Secure Real-time Transport Protocol
SW	Software
TLS	Transport Layer Security
UMTS	Universal Mobile Telecommunications System
USB	Universal Serial Bus
USB-CDC	USB communications device class
VPN	Virtual Private Network
WAP	Wireless Access Point
WiFi (WLAN)	Wireless Local Area Network
WTLS	Wireless Transport Layer Security