



INTERNATIONAL
CRYPTOGRAPHIC
MODULE CONFERENCE 2017
May 16-19 | Westin Arlington Gateway | Washington, DC



Achieving Effective Mobile Security With a Commercial Mobile Device

Richard C. Schaeffer, Jr.

rcschae57@verizon.net

410-703-2928



Customer “Wants”

- Secure Voice, Video, Messaging
 - Controlled Unclassified Information (Sensitive But Unclassified)
 - SECRET
 - TOP SECRET
- A true Commercial Mobile Device (CMD)—Smartphones & Tablets
- Ease of use
 - Scalable architecture that leverages, to the maximum extent possible, available commercial components, including edge devices
 - Extensible to coalition and partner operations
 - Ability to deny adversarial benefit from lost or compromised devices
 - A single device for personal and operational use

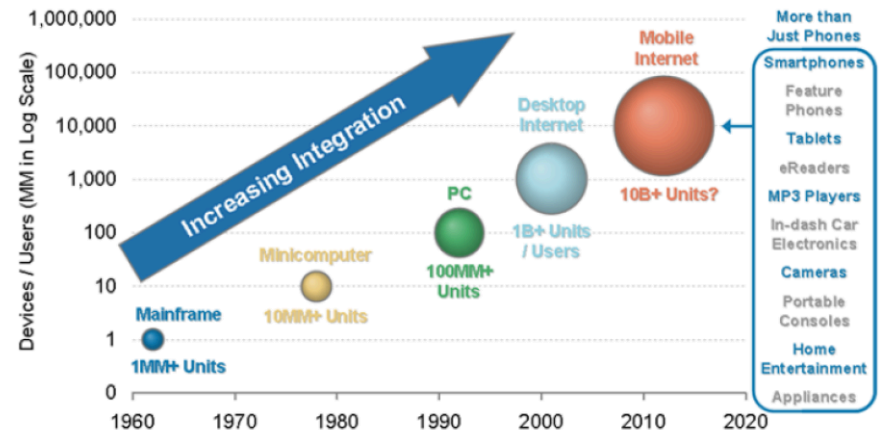


The Problem

- How to leverage one of the most game changing technologies in history—it has changed the way we communicate and the way we operate
- Secure User and Operational data to the Secret and Top Secret Level on a purely commercial device
 - High security has been one of the most illusive tasks for security engineers
- Despite the USG & world enterprise efforts, the security gap has no signs of closing

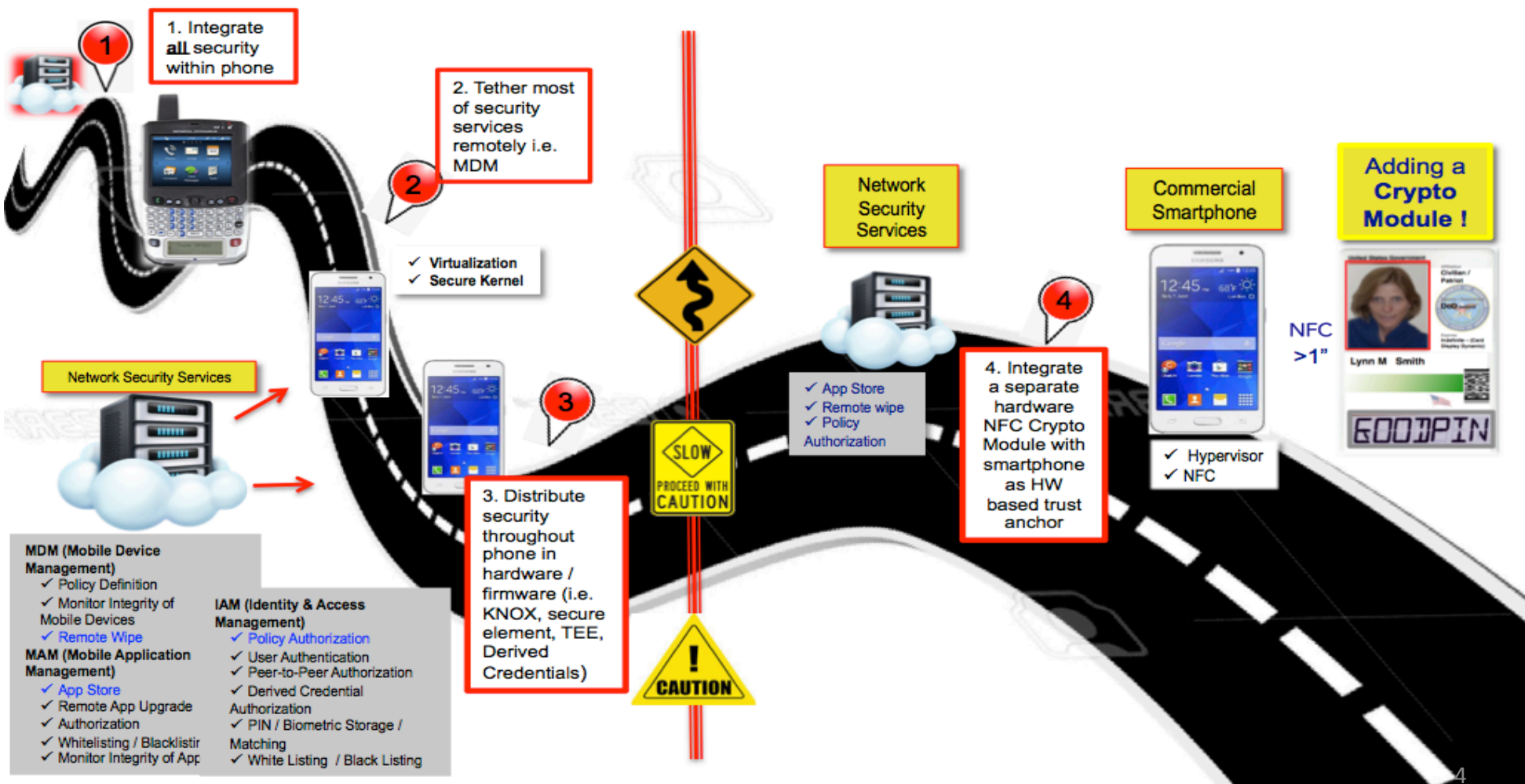
Each new computing cycle typically generates around 10x the installed base of the previous cycle

Devices or users in millions; logarithmic scale





An (Innovation) Road Less Traveled





A Powerfully Different Approach

1

Integrate **all** security within phone



- ☐ 2 year development
- ☐ 5 – 30 times more \$\$\$
- ☐ Custom network infrastructure
- ☐ Difficult to expand
- ☐ Not interoperable
- ☐ Not leveraging commercial

- ☒ Meets Secret / TS Data security requirements
- ☒ Data-at-Rest

2

Tether most of security services remotely i.e. MDM



- ☐ Prone to large attack vectors – easy to exploit via expanding phone capabilities
- ☐ Must be physically returned for rekeying / provisioning
- ☐ SBU only
- ☐ No Strong User authentication
- ☐ No HW based encryption

- ☒ Personal & Enterprise data zones
- ☒ True commercial

3

Distribute security throughout phone in hardware / firmware – Refined – best in class security

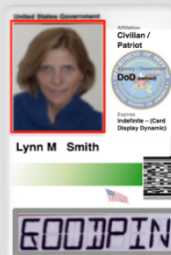


- ☐ Still prone to large attack vectors
- ☐ Must be physically returned for rekeying / provisioning, no OTA rekeying, no remote wipe
- ☐ No scalable Constant Security Health Monitoring
- ☐ Unique solution set for every handset version
- ☐ No Strong User Auth

- ☒ Added secure network gateway
- ☒ Double tunneling
- ☒ Derived Credentials
- ☒ MDM, MAM, & IAM services refined

4

Integrate a separate hardware NFC Crypto Module with smartphone as HW based trust anchor

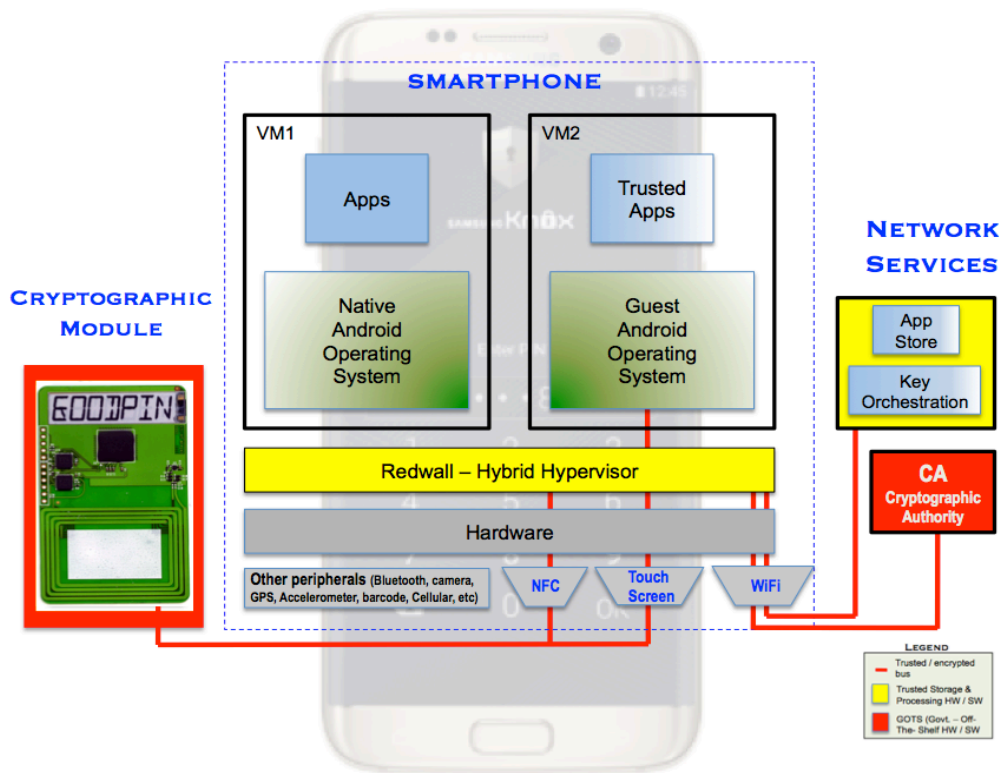


- ☐ Not a stand-alone technology solution, – nevertheless very scalable
- ☐ Should be implemented on select commercial smartphones with trust chains in manufacturing

- ☒ Secret / TS protection using HW Crypto Module as trust anchor
- ☒ Strong 1-2-3 factor user authentication
- ☒ One CM to enable all user devices
- ☒ Data-at-Rest
- ☒ Mission, role, privileged selectable
- ☒ OTA rekeying, remote wipe, secure auditing, Continually security health monitoring



A Novel Architecture



- We realized that the Tocreo Crypto Module (TCM) is not the only component needed to fully protect the mobile device—a Hybrid Hypervisor is an essential component

The resulting solution provides a suite of services including:

- Device / User Authentication, including Role-Based authentication and Peer-to-Peer authentication
- Cryptographic-based unlock key for a *Trusted Workspace* and applications
- Isolation of workspace, applications and data at different levels of classification or sensitivity
- Derived Credential key generation
- Continuous Security Health Monitoring and Attestation of the mobile device
- Secure Boot up of the mobile device
- Rapid Provisioning and Over the Air (OTA) rekeying
- Audit logs of all transactions captured in the TCM memory

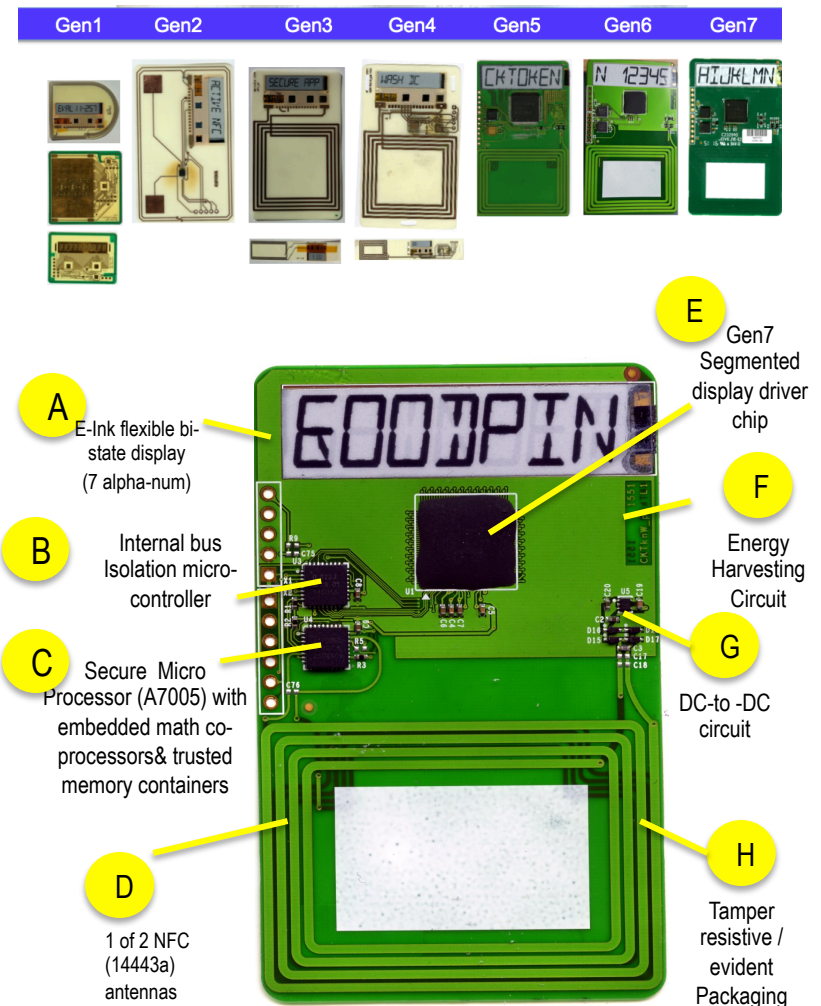


Impact on Operations



Milestones

- Not an overnight success – 7 Generations in 5 years to achieve a fully functional and producible Crypto Module
- Not just a memory card – **secure processing, memory and display** on a thin-film substrate
 - Fully programmable processor – Suite B implemented
 - Bus isolation processor
 - Trusted memory
 - Bi-State display
 - Energy harvester
- Bus isolation processor enables the Crypto Module to become the master device – isolates the Crypto Module Trusted Execution Environment
- Parasitically powered via a commercial NFC interface in the mobile device
- Encapsulation process yields a Tamper-Evident module





Summary

- We developed an innovative approach to a *long-standing* challenge in the Secure Mobility space
- The Tocreo Crypto Module described in this presentation is a game-changing technology
- We are prepared to demonstrate the aforementioned capabilities TODAY





INTERNATIONAL
CRYPTOGRAPHIC
MODULE CONFERENCE 2017
May 16-19 | Westin Arlington Gateway | Washington, DC



THANK YOU!

Questions?



Near Field Communications (NFC)

3 Modes of Operation
In NFC Standard



Power is coupled into card via Magnetic Induction

- Carrier Freq. 13.56MHz
- Short range > 1 inch (15cm) – touch
- Data Rate - 212Kbits = 2-way communication
- NFC will be in +90% smartphones by 2018



NFC was designed
to power simple
memory tokens . . .

NOT

. . . Complex Cryptographic Modules
with Flexible Displays, Security
Processors, Trusted Memory, & I/O

Or so they thought!