



Towards An Intuitive Mobile Security Solution

Attaining Best-in-Class Mobile Security



Carl L. Nerup
cnerup@cogsystems.com

Dr. Daniel Potts
danielp@cogsystems.com

Abstract

Facing today's mobile security threats is daunting. Discovering the right mobile security solution shouldn't be. This white paper explores today's threat landscape for smartphones and tablets, examines costs from security exploits and breaches and compares approaches to securing off-the-shelf mobile devices. Finally, it presents a new mobile security solution, including path to market and options for monetization by mobile ecosystem participants.

CONTENTS

Introduction	2
Today's Mobile Cyber-Security Landscape.....	2
The Real Cost Of Vulnerability	3
Mobile – The New Corporate Desktop PC	4
The Mobile Software Lifecycle.....	5
Meeting Corporate And Government Requirements.....	6
Paths To Market.....	6
Introducing D4 Secure.....	7
An Intuitive COTS Solution To A Bespoke Problem	7
D4 Secure Architecture.....	8
D4 Secure Core Features	8
D4 Secure Differentiating Capabilities.....	9
In-Channel And Field-Based Enablement.....	9
Monetization - Additional Revenue Paths For Device Oems.....	10
Conclusion	10

Introduction

Today's mobile security landscape is nothing short of dire. Unsecured mobile platforms, platform fragmentation, under-curated mobile application stores, unprecedented proliferation of mobile malware (including industry-specific malware) threaten to turn personal and professional productivity devices into the digital plague carriers of the twenty-first century.

The entire mobile ecosystem is investing R&D, engineering and integration resources into making current and next generation devices more secure. Facing down the security onslaught, however, is more than an exercise in cumulative technological will. It requires a nuanced view that spans from chipset providers and device manufacturers (OEMs) to mobile operators to devices and services channels to end-users. It begs a cross disciplinary approach that combines existing technologies to deliver an intuitive solution that accommodates and enhances business models instead of disrupting them.

Even if today's mobile security threats are daunting, discovering the right mobile security solution shouldn't be. This white paper explores today's threat landscape for smartphones and tablets, examines costs from security exploits and breaches and compares approaches to securing off-the-shelf mobile devices. Finally, it presents a new mobile security solution, including paths to market and options for monetization by mobile ecosystem participants.

Today's Mobile Cyber-Security Landscape

Threats to mobile devices have taken on both historic qualitative and quantitative dimensions, unseen even in the heyday of Windows desktop PC malware infestations. The present situation is indicative of a multi-year distressing trend: the mobile marketplace continues to witness an astonishing uptick in

- Malicious email attachments and MMS payloads
- Malware evading app store curation, in particular for Android
- Rampant growth in ransomware
- Previously-benign (if annoying) adware taking on a more sinister character, e.g., using privilege promotion to display aggressive and increasingly malicious advertising screens
- An increase in reported vulnerabilities in key web/mobile components, exemplified by "StageFright" (CVE-2014-7915/7916/7917, 2015-0829/1538 and others) targeting Android
- Emergence of new (innovative) social engineering techniques, e.g., SMiShing (phishing using SMS text messages)
- Retail sale of mobile hacking tools, including Remote Access Tools (RATs) and accompanying administrative platforms to operationalize hacking activities
- A worldwide spike in total mobile malware inventory (see Figure 1.)

In terms of absolute numbers, 2017 was a banner year for mobile security threats, according to McAfee:

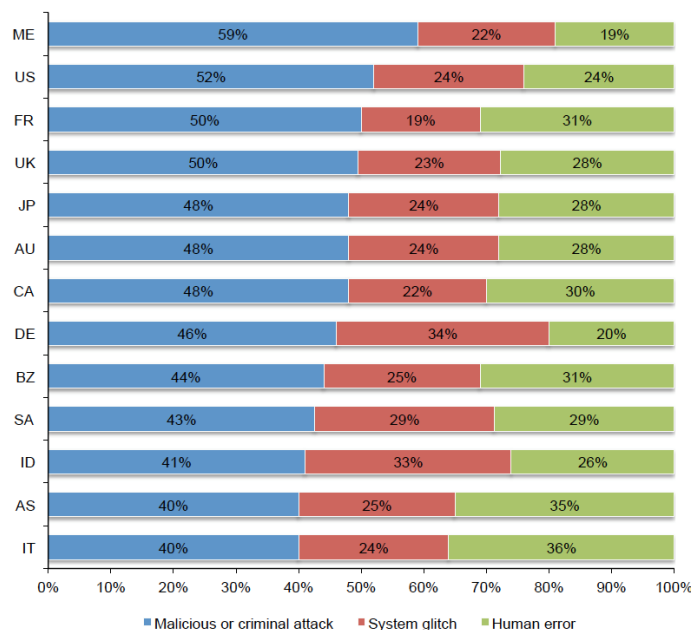
- Total mobile malware grew 56% in the past four quarters to 21 million samples.
- New mobile malware jumped by 60% in Q3, fueled by a big increase in Android screen-locking ransomware.
- New ransomware rose by 36% in Q3, boosted by a big increase in Android screen-locking threats.

The Real Cost of Vulnerability

Economists struggle to quantify the real costs of security threats and actual breaches to companies and to national and international economies. Self-reported costs from cybercrime show the greatest impact falling upon the middle market, where the scope of threat is comparable to enterprise IT, but SMB security budgets are proportionately (and absolutely) smaller than those in major enterprise settings.

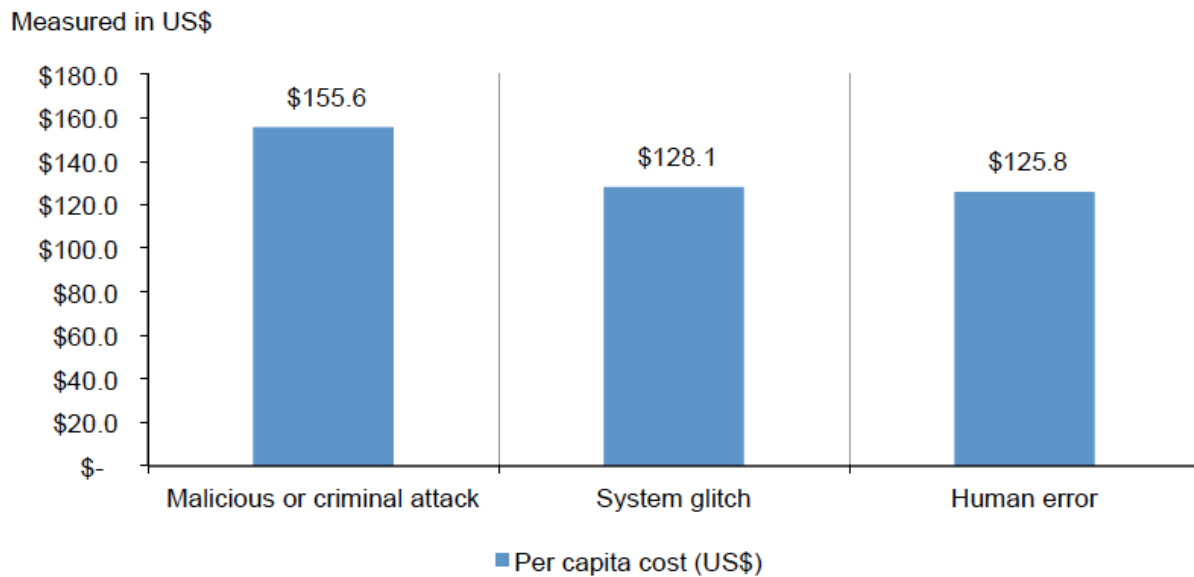
- Cyber crime damage costs to hit \$6 trillion annually by 2021 (Cybercrime Report 2017, Cybersecurity Ventures)
- The most costly cybercrimes are caused by denial of service, malicious insiders and malicious code. These accounted for more than 59 percent of all cybercrime costs per organization on an annual basis (Ponemon Institute)
- Global ransomware damage costs are predicted to exceed \$5 billion in 2017. That's up from \$325 million in 2015—a 15X increase in two years, and expected to worsen. (Cybercrime Report 2017, Cybersecurity Ventures)

Figure 1. – Per capita cost for three root causes of data breach by country and region (Ponemon)



Malicious or criminal attacks are the lead cause of data breaches. These costs impact business in a variety of ways, including disruption of operations, loss of information, equipment damages and outright loss of revenues.

Figure 2. – Per capita cost for three root causes of the data breach (Ponemon)



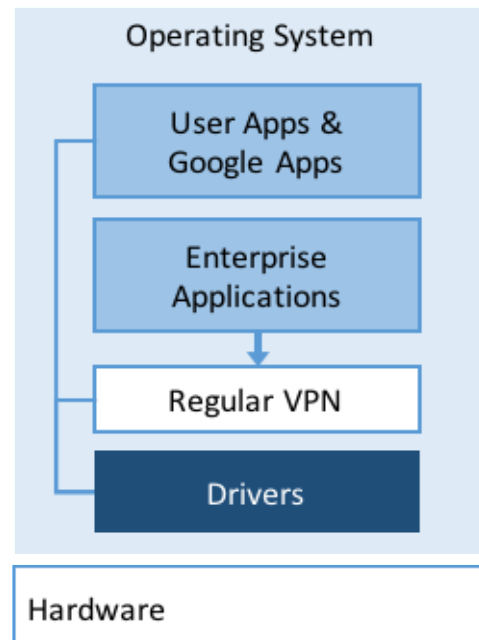
Mobile – the New Corporate Desktop PC

Security-wise, your mobile device is the new desktop PC. And not in a good way. A decade ago, the desktop PC was the focus of pain for enterprise IT. PCs were highly stateful, increasingly connected and presented multiple vulnerable attack surfaces, leaving them completely exposed.

Today, mobile devices fulfill many of the same roles as desktop computers. Smartphones and tablets support off-the-shelf applications for productivity, host enterprise application clients, provide connectivity to email, the web and to enterprise resources. In serving desktop-equivalent missions, they also boast increasingly impressive specs, with substantial processing power, storage and network connections.

Moreover, they are being increasingly used as a platform for new applications as we use them to interact with our connected world. We will increasingly see them being used to interact with or even perform a critical safety, reliability, or security function like those in IoT, medical, automotive, etc. Many people are already using mobile devices to interact with their IoT appliances, cars, and other devices.

Figure 3. Android App Context



Mobile devices face comparable threats, from malware and ransomware, phishing, spoofing, man-in-the-middle and DDoS attacks, to name but a few. And so, smart phones and tablets need the same (or better) protections as their desktop predecessors.

Unfortunately, mobile platform designers and application developers continue to follow tried-and-true monolithic design patterns. The dominant OS, Google's Android™ (with Linux at its core) comprise massive, vertically integrated software stacks. Google has been continuously adding in new security features to improve the security posture of Android devices with features that protect applications, including SE for Android policy, and full disk encryption. The Android RunTime (ART) executes each application in its own process but because it shares other resources, like VPNs, storage and devices, Android applications are hardly more robust or secure. Underneath the applications remains a large attack surface inherent in a monolithic system. Despite on-chip virtualization support and other capabilities, Android apps and services enjoy no further hardening or isolation. For its part, Samsung KNOX adds defense-in-depth by leveraging ARM TrustZone, but has done little to the OS architecturally.

The Mobile Software Lifecycle

The mobile software lifecycle differs in important ways from the enterprise desktop, most notably in mobile operators exercising control over the platform/OS vs. IT departments. With the ability to configure the underlying OS, security software vendors have been limited to after-market, application-level solutions that rely upon, extend and/or attempt to replace mobile OS-native communications stacks, encryption key management, data stores and application containers. The result has been a patchwork of ad hoc security measures and proprietary application containers that require use of custom productivity apps (especially mail clients and messaging apps) and/or vendor-specific APIs and application platforms that present formidable integration challenges. Ultimately, these actually crippled productivity, rather than enhance it.

Instead of technical band aids, what is required to meet the mobile security challenge are intuitive system-level solutions with capabilities that include:

- Multi-layer security, for “defense in depth”
- Pervasive, high-strength encryption, for data at rest (in file systems) and data in transit entering, exiting and traversing communications stacks
- System-native (vs. application-based) VPN, to keep private communications private
- Secure key management, to protect passwords encryption keys, to ensure that one breach doesn't compromise multiple apps and systems
- Isolation of critical security functions

Meeting Corporate and Government Requirements

Another area where existing mobile security offerings break down is in support for and certification of off-the-shelf Mobile Device Management software (MDMs). The MDM category of mobile software has exploded in the last few years, and popular solutions typically include several standard handset-based components supported by data center-based gateways and management portals. Note that as the term would indicate, MDMs aid in managing mobile devices – they do not provide incremental security against today’s threat landscape.

MDM is so pervasive in enterprise IT that both corporate and government requirements have emerged for MDM capabilities, with explicit support for a number of off-the-shelf shrink-wrapped MDMs. Like the list of must-have system-level security solutions in the previous section, MDM support requires access to system-level resources to function correctly, resources inaccessible to after-market MDM offerings.

As such, a viable total mobile security solution should both accommodate and require a set of MDM “hooks” (secure APIs and data structures), accompanied by a global certification program for a set of leading MDM solutions, for installation on mobile devices in-channel or post-deployment (i.e., not at the factory), by operators, integrators and/or enterprise IT staff.

Paths to Market

Another key difference from the desktop PC market is that mobile security solutions follow multiple paths to market:

- OEM-based – integrated together with platform and hygiene/core application set by the handset manufacturer
- In-channel – Installed or enabled by mobile operators, integrators and/or other ecosystem participants
- End-user – Installed or enabled by enterprise end-user IT departments or the end-users themselves

These three paradigms share certain elements and activities, but have very different implications for commercial success and in their abilities to protect devices and enterprise resources:

Figure 4. Comparing Paths to Market for Mobile Security Solutions

	Business Model and Monetization	Upside	Security & Business Challenges
OEM-Based	Cost embedded in BOM Revenues from in-channel / end-user enablement and on-going service	Tightest integration All devices can enable security	Tend to be simple, one-size fits all solutions Limited options for MDM When not used, complicates support
In-Channel	Cost embedded in device sale Revenues from individual or enterprise mobile subscriptions and from management services and portals	Most flexibility Addresses enterprise and SMB use cases	Solutions need to address multiple devices and OS versions Not all devices support in-channel programming
End-User	Retail and/or ongoing subscription cost	Familiar enterprise acquisition model Relatively simple to install on devices	Mostly leverages (weak) OS-native capabilities Implements user-level capabilities (less secure) Complex portal set-up and maintenance Limited choice of MDMs Vendor lock-in

Staying Ahead of Today's Cyberattacks

The mobile IT security threat is daunting. Discovering the right mobile security solution shouldn't be. The right solution starts with an intuitive mobile security solution for OEM integration and in-channel and end-user enablement – the best of all worlds in mobile security.

An Intuitive COTS solution to a bespoke problem

Mobile security solutions can be highly customized, integration-intensive and questionably secure. However, building on a pre-integrated platform and hardware infrastructure that is fully locked down while still customizable is a viable option. By shipping direct from the OEM, this type of mobile security approach offers mobile service providers, IT shops and other parties an unparalleled set of rich capabilities, including certified interoperability with popular MDM and other in-channel security offerings.

Modular vs. Monolithic Approach

A modular approach isolates key components, integrates with MDMs and effectively secures mobile devices. This paradigm shift from a monolithic approach:

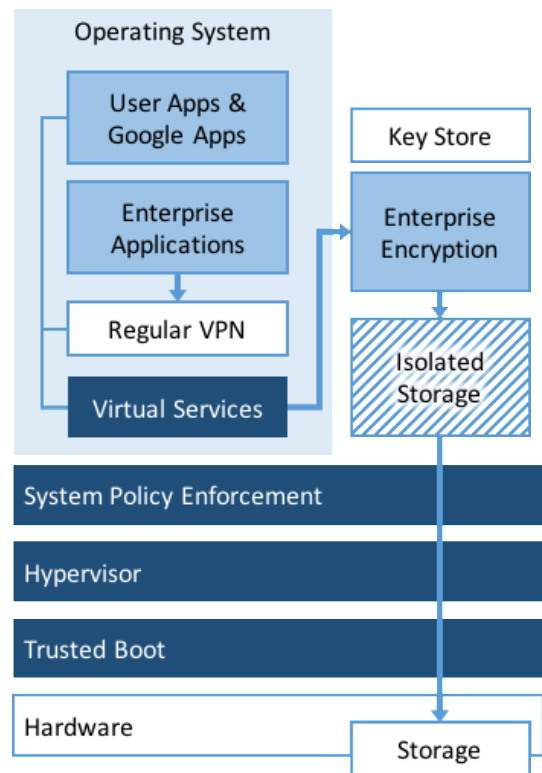
- Leverages Type-1 virtualization (bare metal) to isolate key components, and to enable layering of new components
- Reduces the attack surface through isolation
- Supports greater customization with formal interfaces and the ability to swap components in and out
- Supports feature-rich secure applications (in much the same way TrustZone supports applets)

Modular Core Features

A modular solution addresses the most pervasive and pressing enterprise security requirements with the following capabilities:

- Enhanced Resource Protection – System Policy Enforcement provided outside the OS that enforces a minimal set of access rights across the entire system thereby further protecting Android from certain types of malware.
- Multi-tier data store encryption – implemented for the entire disk/file system with both native OS encryption and root-level AES algorithms
- Industrial strength multiple layer VPN solution
 - Non-By-passable Outer VPN and Mobile Device Firewall – all voice (VoIP) and data traffic passes through a single VPN, enabling full audit communication and internet access control, and eliminating dependencies on third-party MDM software
 - Nested – enabling two, separate and distinct VPN clients on a device – the ‘Gold Standard’ of data in transit protection
 - Multi-hosted – server optionally residing in the cloud or on customer premises
- Isolated Key Store – virtualizing the Key Store and completely segregating it from the mobile OS and applications

Figure 5. Modular Architecture



- Government Certification – certified against NIAP Protection Profiles, and certified for use with the US Department of Defense Commercial Solutions for Classified Program (CSfC) and commercial applications of all types
- Monetization – back-end to support VPN and Call Manager, creating additional revenue partnership opportunities

Differentiating Capabilities of a Modular Approach

Going modular stands out from the competition with an impressive complement of capabilities:

Figure 6. Comparing Modular to Conventional Mobile Security Solutions

	Handset-based	Modular	After-Market
Commercial OS (Android)	✓	✓	✓
Non Bybassable VPN	x	✓	x
Nested VPN	x	✓	x
OS Native VPN	✓	✓	✓
Isolated Outer VPN	x	✓	x
Dual Encryption	x	✓	x
OS Native Encryption	✓	✓	✓
Isolated Encryption	x	✓	VoIP/ Msg Only
Isolated Storage Driver	Container Only	✓	x
Isolated Modem / Wi-Fi Driver	x	✓	x
Isolated Entropy Engine	x	✓	x
Isolated Key Storage	x	✓	x

In-channel and Field-based Enablement

While the modular approach is an OEM-based solution, integrated as part of mobile device bills-of-material (BOMs), devices leave the OEM premises in their generic mass market state. A modular solution has the unique capability of being enabled in-channel by integrators, retailers and by mobile operators to meet the needs of particular regions and segments. The same option exists for qualified end-user organizations who wish to implement BYOD and/or secure company acquired fleets of devices.

- In-channel and field-based enablement offers:
- Maximum flexibility for special use cases and monetization models (see below)
- Granular control of enabled feature sets to suit market and end-user requirements

- Interoperability with and certification of popular MDM suites

Monetization - additional revenue paths for device OEMs

Mobile OEMs traditionally faced a tough choice: create more compelling and useful devices at the factory with new software or cut BOM costs to preserve margin. A modular approach helps OEMs avoid the dilemma by imbuing mobile devices with greater security capability, off-the-shelf, AND providing in-channel and after-market revenue paths. Monetization options include:

- Revenue streams from in-channel and end-user enablement of modular-based services provided by OEMs and/or their channel partners
- Resale and revenue sharing with MDM and other security solutions providers

Conclusion

Government and enterprise can no longer afford to leave their mobile workforce vulnerable to cyberattacks. Today, organizations that transition from reactive mobile security solutions to proactive solutions are better equipped to stay ahead of ongoing cyber threats. It starts by going modular and building in redundancy and defense-in-depth.

Cog Systems delivers on this premise by changing the way we build mobile security systems from an 'old school' monolithic approach to a modular approach. We couple the same modularity techniques used in cloud computing with the fundamentals of security, trustworthiness, robustness and adaptability to proactively create highly secure connected devices.

This unique approach provides the assurance of defense grade security so our customers can focus on delivering best-in-class applications, performance and usability.

Contact us today for a demonstration of our D4 Secure modular solution.

Phone: U.S. +1 855-662-7234 Australia: +61 2 9018 1077

Email: info@cog.systems