THE EMERGENCE OF SECURE MOBILITY EBOOK

PRIVORO®

SMARTPHONES: UBIQUITY, UTILITY AND A RISK TO NATIONAL SECURITY

As mobile devices surpass traditional computers as the dominant mode of computing, malicious actors increasingly focus their efforts on these devices. The smartphone's huge attack surface gives hackers virtually unlimited ways to gain illicit access. Once in, hackers can use tools like rootkits and remote access Trojans (RATs) to take over these devices and siphon their data, including taking control of smartphone cameras and microphones to eavesdrop and spy on everything around the phone.

THE ENTIRE SMARTPHONE ECOSYSTEM IS VULNERABLE TO COMPROMISE

Smartphones are vulnerable at every layer, making them prime targets for threat actors. After compromising a device, these exploits may be leveraged to hijack the cameras and microphones – turning the smartphone into a surveillance device.

Software alone is not enough

Software-based security makes a flawed assumption – that it can detect malicious software operating at the same or lower level in the smartphone ecosystem.

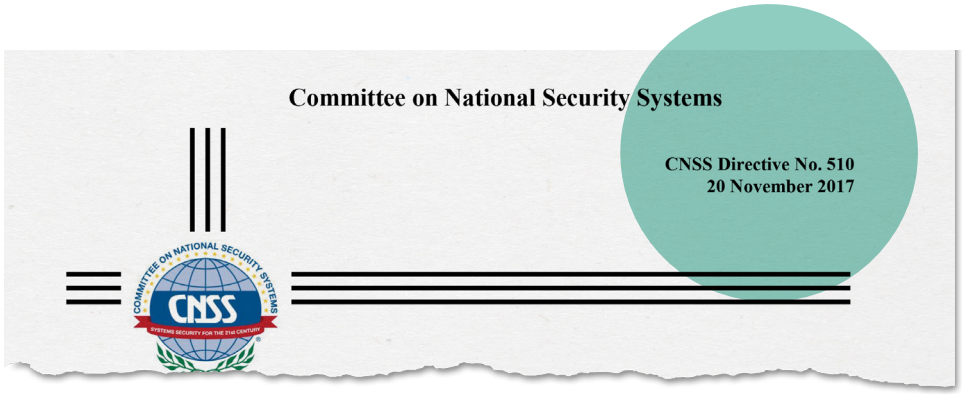
Separate hardware is required

With mobile exploits capable of gaining control of the entire smartphone, including at the hardware level, only external, device-independent hardware can be trusted to provide security.

PRIVORO®

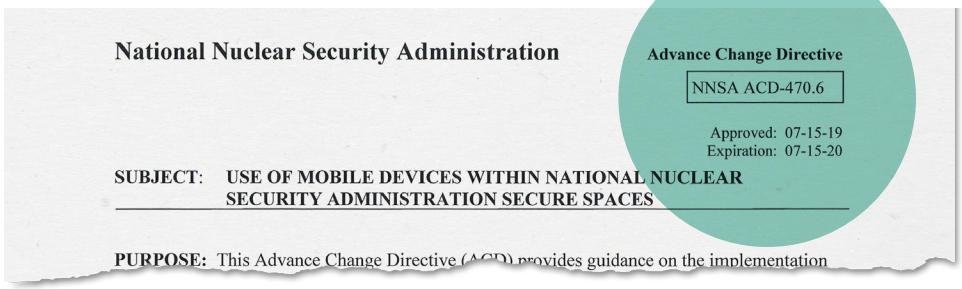
MITIGATING THE INHERENT RISKS OF COMMERCIAL MOBILE DEVICES

As many U.S. Government Agencies and Departments rely on mobile technologies to increase productivity and mission flexibility, these same devices pose significant risk to National Security Systems when introduced into secure spaces and ultimately, any place sensitive information is discussed or presented. As a result, many of these same organizations have established requirement directives in an effort to minimize the risk of mobile espionage. These include:


Committee on National Security Systems

CNSS Directive No. 510
20 November 2017

- Committee on National Security Systems: CNSS Directive 510: Directive on the Use of Mobile Devices Within Secure Spaces


National Nuclear Security Administration

Advance Change Directive
NNSA ACD-470.6

Approved: 07-15-19
Expiration: 07-15-20

SUBJECT: USE OF MOBILE DEVICES WITHIN NATIONAL NUCLEAR SECURITY ADMINISTRATION SECURE SPACES

PURPOSE: This Advance Change Directive (ACD) provides guidance on the implementation

- National Nuclear Security Administration Advanced Change Directive: ACD 470.6 Directive on the Use of Mobile Devices Within Secure Spaces

These directives include a requirement of securing and monitoring smartphone cameras and microphones to prevent unwarranted surveillance and interception of data in vicinity of these devices.

WHAT'S AT RISK?

The collection of data in vicinity represents one of the greatest risks for government agencies charged with operational security and mission effectiveness.

NATIONAL SECURITY INTERESTS

MILITARY OPERATIONS

INFORMATION GATHERING

RELATIONSHIPS AND AGREEMENTS WITH OTHER

GOVERNMENTS POLICY DISCUSSIONS

THE DOWNSIDE OF SMARTPHONE BANS

Recruiting challenges:

4 out of 10

millennials refuse to work for an organization that doesn't allow personal devices in the workplace.

Source: 2016 Economist Intelligence Unit survey

Decreased morale:

60%

of federal agencies have declining employee engagement scores.

Source: 2018 Partnership for Public Service survey

Lower productivity:

52

minutes of productivity time are lost per day due to not having a smartphone at work.

Source: 2016 Frost & Sullivan survey

Security risks:

2 out of 5

federal employees are willing to sacrifice government security in order to use a mobile device at work.

Source: 2015 Market Cube survey

PRIVORO®

THE PRIVORO SOLUTION

The Privoro SafeCase – a first-of-its-kind ExoComputer for mobile devices – provides integrated protections against audio and video surveillance and cloud-based policy management tools for administrative oversight of SafeCase policy.

SAFECASE

CLOUD

IOS APP

SECURE DATA CHANNEL

PRIVORO®

MEETING SPECIFIC COUNTER-ESPIONAGE REGUIREMENTS: MOBILE HARDENING

Mobile Hardening

Privoro provides the only hardware-based solution to the requirement of safeguarding smartphone cameras and microphones from unwarranted surveillance – also known as mobile hardening. For this reason, SafeCase is currently being piloted across a range of Federal Agencies and Departments.

PROTECTION AGAINST AUDIO AND VIDEO SURVEILLANCE

The Science of On-Device Audio Masking

Proprietary audio masking technology works by adding randomized noise to each of the associated mobile device's microphones, safeguarding both the content and context of conversations.

Physical Camera Blocking

The hood on the SafeCase acts as a physical barrier covering each of the smartphone's cameras – preventing intruders from observing or recording any visual data in the device's vicinity.

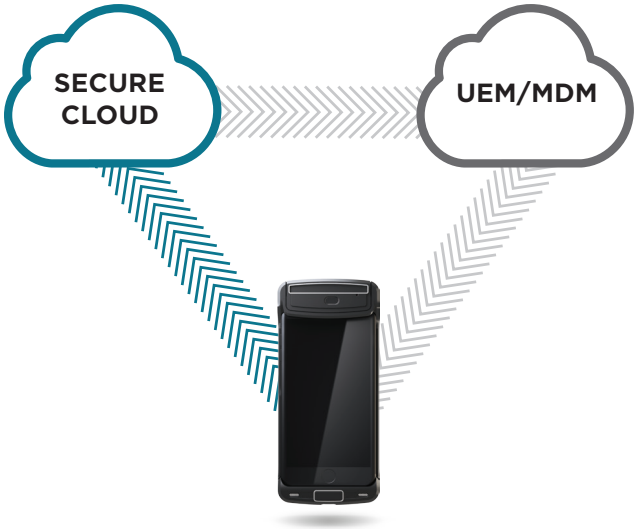
FROM SYSTEM ARCHITECTURE TO MANUFACTURING, SECURITY DRIVES EVERY FACET OF THE SAFECASE SOLUTION

PRIVORO SECURE MANAGEMENT PORTAL

Configure and Monitor Policy Based on SafeCase Actions

Administrators can specify when and where smartphone cameras and microphones may not be exposed through geofences established in the portal.

EXTENDING POLICY COMPLIANCE VIA UEM/MDM INTEGRATIONS



By integrating the Privoro policy engine with an organizations Unified Endpoint Management (UEM) or Mobile Device Management (MDM) solution, sysadmins have the ability to enforce policy compliance via actions taken directly on the associated mobile device.

PRIVORO®

The Emergence of Secure Mobility

PRIVORO SAFECASE: HIGH-SECURITY PROTECTIONS AGAINST MOBILE ESPIONAGE

The Privoro SafeCase is the only hardware-based solution enabling government organizations to achieve high-security mobility, mitigating the risks and limitations of commercial mobile devices.

PRIVORO®