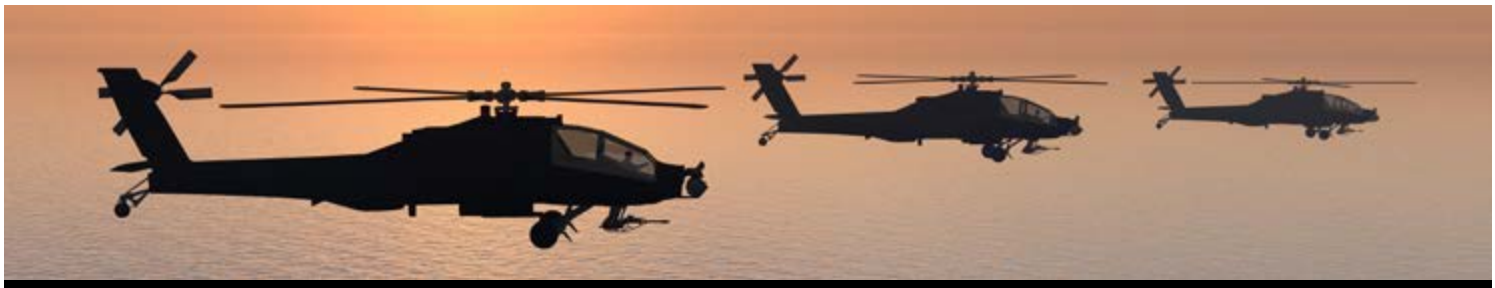

Safeguarding the sensitive and classified information of military and government personnel in a mobile environment.

Situation Summary: Military and government personnel are targeted

1. Generally considered high-value targets given the roles, responsibilities and access to knowledge/information.
2. Face the most sophisticated, capable, well-funded and determined attackers. It is the dedicated focus of other nation states, including allies to gather this information.
   - "Inside the OPM Hack, The Cyberattack that Shocked the US Government" –*Wired,* October 2016
3. Many examples, including:
   - "Hackers are using this Android malware to spy on Israeli soldiers": Malware which can: "*... eavesdrop on conversations and perhaps most importantly for the perpetrators - take photos at any time.*" –*ZDNet,* February 17, 2017
   - "Operation Pawn Storm": "*Creating (and using) iOS malware for espionage ... steals all sorts of information from the mobile device it infects, ... geo-location data, pictures and even voice recordings.*" Targets: Military, Defense, Government & Other –*Trend Micro,* January 16, 2016
   - "North Korea denies cyber attacks on South Korean officials": "*North Korea had recently stepped up cyber attack efforts against the South and succeeded in hacking the mobile phones of 40 national security officials*" – *VentureBeat,* March 13, 2016
   - "Danger Close: Fancy Bear Tracking of Ukrainian Field Artillery Units": *"Open source reporting indicates that Ukrainian artillery forces have lost over 50% of their weapons in the 2 years of conflict and over 80% of D-30 howitzers" –Crowdstrike,* December 22, 2016
   - "Secret Back Door in Some U.S. Phones Sent Data to China": *"...preinstalled software in some Android phones that monitors where users go, whom they talk to and what they write in text messages."* –*NY Times,* November 15, 2016

The Problem: Smartphones are inherently vulnerable to attack

1. Long supply chain: Many components come from and assembly is often performed in Asia, which carries risks for government, intelligence, military and defense contractor personnel.
2. Large attack surface
   - Browser: Capable of accessing the entire internet, including malicious sites.
   - App development platform: Previously compromised/ attacked. Millions of apps with risk from both the malicious as well as the legitimate (that over-reach in their data collection).
   - General-purpose operating system: Supporting many features, functions and services, all of which may be attacked.
   - Android: Highly fragmented marketplace, resulting in poor software hygiene/updates/security.
3. Incentive: Getting into your phone is a highly profitable business
   - Crack Apple iOS, access some of the most sensitive info for 500+-million users.
   - "Battle Heats Up Over Exports of Surveillance Technology": *"The interception industry is growing rapidly, with worldwide sales estimated to reach $1.3 billion by 2019, according to Markets and Markets, a research firm." –NY Times,* October 31, 2015
4. Sophisticated, well-funded and determined attackers:
   - Nation states have dedicated teams per platform, spend enormous amounts of money pursuing and are capable of intercepting, interdicting or compromising the supply chain.
   - 20+ commercial companies dedicated to developing mobile malware.
5. Smartphone security software does not solve the problem. Security at any level loses to attacks at a lower level (i.e., apps lose to operating system lose to firmware lose to chip) and the entire stack has been proven to be compromised.
   - Millions Of Smartphones Using Broadcom Wi-Fi Chip Can Be Hacked Over-the-Air –*The Hacker News,* April 4, 2017

Intelligence collected by smartphones can be extremely sensitive/damaging

1. People have sensitive conversations outside of a SCIF. Confidential information will come out in normal conversations with people they trust.
2. Audio eavesdropping can reveal strategies, plans, deployments, etc.
3. Cameras can reveal sensitive info (e.g., inside of nuclear submarines, classified facilities, locations, relationships).
4. RF emissions can reveal troop stationing and movements, ship locations, meetings, individual movements, habits and relationships/associations (opening people for compromise or targeting), building or base layouts, etc.

Privoro Privacy Guard: Overview

1. Prevents smartphones from being used as surveillance devices, even if they have been hacked.
   - All 4 sensitive microphones on the phone are independently and securely jammed.
   - Both front and back cameras are covered.
2. Selectively prevents location tracking or attacks via the RF layer:
   - Applying Privacy Guard cover creates a high-performance Faraday cage around the phone.
     - — The phone's RF footprint/emissions are massively reduced (or essentially eliminated) from detection.
     - — The ability of external signals (e.g., cell tower transmissions, WiFi, etc.) to reach the phone are similarly reduced/eliminated.
3. Easy to use.
4. Air-gapped, hardened platform: Airgap prevents remote access to Case's chips/firmware. Tamper resistance restricts access to internal components and helps make tampering visible/evident.

Military awareness of mobile surveillance is increasing

1. "Army says smartphone, digital tech increase vulnerability": *"…the Army fears that its massive electronic footprint is becoming a major vulnerability that could leave troops more exposed and open to detection. Electronic signals emitted by U.S. forces make it easier for tech-savvy enemies to keep tabs on units' locations and movements. The spying tools are relatively cheap and ubiquitous: iPhones, Google maps, commercial tracking software. 'It's an unbounded battle space,' said Lt. Gen. Robert Ashley Jr., Army deputy chief of staff for intelligence. The idea that anywhere the Army goes there might be people out there 'pushing pictures' fundamentally undermines 'our ability to have operational security.'" –Defense Systems,* May 9, 2017
2. "General: Marines, put down those cell phones!": *"Neller said the Marines and Navy had seen exercises in which their personnel's use of mobile devices could give away positions to adversaries. 'What do you think the largest electromagnetic signature in the entire MEF headquarters emanated from? The billeting area. Why? Because everybody had their phone on. The Navy has come up with plans to reduce its reliance on modern electronics to make its force harder to trace, going so far as to have sailors re-learn navigating by the stars instead of using the Global Positioning System', he said." –CNN,* August 11, 2016
3. NATO, allies in major drill at Estonia cyber range to ward off malware, infected devices" *–U.S. News & World Report,* November 19, 2015
4. "China's military bans Apple Watch": *"The Asian power's military has banned the smartwatch and other wearable technology over cybersecurity concerns that the devices could be used to track troops, record audio and video and capture military secrets." –The Hill,* May 12, 2015

Military and government personnel at highest need for protection

1. Government officials, Intelligence officers and senior military leaders, as well as their aides/staff should have the Privacy Guard case on their phone to protect against the risk of audio and video surveillance.
2. Personnel who discuss and disseminate sensitive information should have the Privoro case on their phone to prevent the compromise of operational security (e.g., talking to spouse about deployments).
3. Any individual whose device can emit an RF signature that can be detected to reveal troop or asset location should have the Privacy Guard case and cover to selectively reduce their RF emissions from being detected.

PRIVORO®