SECURITY EXECUTIVE COUNCIL
A research and advisory firm

Solution Innovation Case Study:
Improving Mobile Communication Security and Safety

The Security Executive Council (SEC) Solution Innovation Partner (SIP) program evolved to help security practitioners expedite choosing a trustworthy risk mitigation vendor with confidence given the myriad of viable options in the marketplace. Proven Solution Innovation Case Studies help to evaluate performance claims and differentiate security solution providers for business outcomes including risk mitigation, return on investment, and security assurance.

This case study demonstrates the Pate Group's Integrity Systems Communications innovative capabilities to address the persistent risks and threats to securing mobile communications (voice, chat, text, and email), the actual users, mobile phone leakage, and AdTech location tracking. The Integrity Systems communications solution is a complete integration of "Commercial Off the Shelf" (COTS) technology that fully addresses the mobile communications issues listed here.

Risk Issues and Mitigation Opportunities:

- Fully secure, encrypted mobile communications platforms that do not look like "special" phones were not truly available.
- Currently used phones like Apple & Samsung leaked data and created an electronic trail.
- Use of multiple "Burner" phones completely dependent on area of operations, meaning these phones would need to be purchased in those regions.
- AdTech tracking via currently utilized mobile phone manufacturers like Apple & Samsung- these companies bring in millions in revenue from allowing AdTech to function on their phones, so they have zero interest in limiting or controlling the AdTech that will identify US personnel and/or their global locations.
- Masks the mobile user's actual location in the global areas of operation.

Solution Requirements:

A secure, 256 end-2-end, encrypted mobile phone that:

- Is a commonly used cellular platform that does not look different or special.
- Does not flag the phone by indicating the phone is using an operating system other than the original
- Does not leak data or create an electronic trail.
- Allows multiple secure/covert "virtual" phones or containers combined within a single mobile phone, thereby negating the need for "burner" phones.
- Allows switching between the "virtual' phones or containers within a matter of seconds w/ each container utilizing an isolated, encrypted file system that is unlocked via a container-specific PIN, password or via biometrics.
- Has the ability to assign multiple non-attributed cell numbers from various regions based on the operational requirements for each team and its members.
- Has the ability to obfuscate the Int'l Mobile Equipment Identity (IMEI) of the phone and "roll" the Int'l Mobile Subscriber Identity (IMSI) based regions of operation ("DoD/USG Only" upgrade).

- Can use E-SIMs or standard SIM cards.
- Can be remotely managed and customized for a specific use-cases including apps, allowed app sources, user authentication, VPN, and access to modems, sensors, & location
- Allows each container to be independently wiped or the device (e.g., all user data) may be wiped via a factory reset triggered remotely or by the end-user.
- Allows containers to also be temporarily removed from the device and stored in a private cloud and later restored to a device for example, to enable a user to access sensitive work apps and data while overseas without risking discovery at a border crossing or airport checkpoint.
- Allows complete control over how cellular devices behave, with options to implement a variety of device controls, such as app install whitelists and blacklists, and always-on VPN implementation.

Delivered:

The Integrity Systems Communications (ISC) -Pro (Application only- BYOD; delivered and implemented with the customer 100% remotely) and the ISC-Guardian- complete secure, encrypted mobile phone package specifically addressed all bullet points in the previous solution requirements section and provides:

- Superior security, easy to deploy, manage, use, and support.
- E2E encrypted text, voice, video, and file sharing between Trusted and Authenticated users
- Encrypted global out-of-network calling & SMS with unique non-attributed, private, and temporary numbers.
- Customizable user status messages for business continuity
- Masks the identity of mobile communication endpoints from others.
- No personally identifiable information (PII), such as name, email, or phone number required.
- An enterprise solution via our data entry point solution to seamlessly secure communications via tablets, laptops, and desktops
- Secure connection for enabled cameras, and sensors
- Use within the HNW/F100 communities, DoD, and various USG Agencies
- Integrated access control, app mgmt. and multi-platform endpoint mgmt. to deliver any app simply & securely on any critical device e.g., mobile, tablet, laptop, and desktop.
- Remote wipe capability
- Configurable, historical dashboards
- Risk analytics
- Private enclaves, which allow a group or organization to have a dedicated secure, private cloud server that cannot be accessed by outside personnel.

Mobile Threat Detection: (iOS, Android, and Chrome OS)

- Cloud-delivered mobile security
- Endpoint detection and response built by threat researchers.
- Meet compliance requirements while preserving user privacy.
- Optimized lightweight app for processor performance and battery life.

- Scales to mobile fleets of hundreds of thousands of endpoints
- Frictionless deployment on all client devices

Outcome and Benefits of Service Including ROI:

Unfortunately, due to the actual client agency requirements, this information is not fully available due to current classification, however:

1) The ISC Suite has reduced necessity for "burner" phones and/or the need for two phones (one official issued phone and one personal), in the various global regions of operation, thereby effecting cost reduction across the enterprise.
2) The ISC Suite continues to meet or exceed current operational requirements within multiple Dept of Defense (DoD), Intelligence Community (IC) small, deployed teams and/or US Gov agencies, HNW Family Offices and F100 Organizations
3) The ISC Suite is the only secure mobile communication package that has been fully tested, vetted, and validated on five levels: operational, technical, functional, vulnerability and intelligence during Trident Spectre 2022- the current classified validation exercise for US Naval Special Warfare, other US Special operations Forces, the US Intelligence Community (IC), and other US agencies. The ISC Suite has been recommended for adoption across the entire US IC and is being evaluated & considered for purchase across the entire US Special Operations Forces (SOF) Community.

SIP Case Study Authentication Process

This process was overseen by a Security Executive Council subject matter expert with 20+ years of experience in developing and leading people and asset protection programs as a trusted security advisor for global, multinational organizations.

Client end-user authenticated by Eric "Pappy" Kleinschmidt, Master Chief SEAL, US Navy (Ret).:

> During the last 20 years, as Special Operations Force (SOF) Sensitive Activities missions have increased, so has the need of the DoD for secure mobile communications. My specific background in generating special communications requirements is very diverse. Having been tasked with solving security vulnerabilities and generating requirements for the National Mission Force's Sensitive Activities Branch in the early 2000's I have come across many methods and/or attempts at solving these problems, many of these same problems are addressed above in the "Problems" and "Requirements" section of this document.
>
> After leaving the National Mission Force, I became the Senior Enlisted Leader/Advisor for Requirements and Acquisitions for the entire East Coast SEAL Enterprise. It was during this time that I came across the Integrity Systems Communications Suite technology during Trident Spectre 2021,

while the ISC Team was attending as a guest of one of my other sponsored solutions providers being evaluated.

Based on my experience and difficulty finding a complete solution to the current secure mobile communications problem set, I immediately tasked my Combat Communications Command to conduct a Test and Evaluation of up to 30 mobile phones utilizing the Integrity Systems technology in the fall of 2021. Although many of the details are currently classified, concerning how and where these phones have been tested, evaluated, and deployed, I can say that the special operators that conducted the evaluations confirmed that the ISC technology did in fact solve a majority of the "Problems" and "Requirements" listed previously in this document and the ISC Team was invited to submit for assessment during TS22.

- During Trident Spectre, an advanced assessment request by any company consists of the maximum number of assessments that may be requested and completed for each company. The ISC Team requested the advanced assessment, which shows the government they have confidence in their technology and that it is at a mature state. These assessments consisted of the following types, and the results and feedback have been provided to the ISC Team.
  1. Technical (Does the technology do what it says it can do)
  2. Vulnerability (Is the technology susceptible to weaknesses)
  3. Functional (How difficult is the technology to operate)
  4. Operational (Technology is handed off to Operational Units to use in the field)
  5. Intelligence (Technology contributes to the Theater and National Intelligence Priority Information Requirements)
- As a Co-Sponsor along with the Defense Intelligence Agency (DIA) for the ISC Suite at Trident Spectre 22, I can attest to the fact that this technology performed extremely well during all assessments.
- 370 companies applied for Trident Spectre 22, only 75 projects to include the ISC Suite were approved and accepted.
- The ISC Suite was one of the first and only approved for secure communications (this is not the norm for a first-time applicant)
- I retired shortly after Trident Spectre 22, and due to the classification assigned to secure communications, I cannot discuss current acquisitions, operational use, or specific deployments but I can say this technology was recommended for adoption across the SOF & Intel communities.

DATE VALIDATED - November 2023.

Note: *The Security Executive Council's Solution Innovation case study represents a snapshot in time to demonstrate a solution to a specific organization's issue. End-user diligence, trial and measurement are strongly recommended for any contemplated risk mitigation activity.*

SECURITY EXECUTIVE COUNCIL
A research and advisory firm

Solution Innovation Case Study:
Improving Mobile Communication Security and Safety

A General Comparison of Competition

Client Service/Resource Attributes or Capabilities	Pate Group-Integrity Systems YES/NO	Secure Mobile Application A YES/NO	Secure Mobile Application B YES/NO	Secure Mobile Application C YES/NO	Remote Secure Comms Company D YES/NO
Open Source client & Server	YES	YES	NO	YES	YES
Virtual option for solution delivery and implementation (for Application only)	YES	YES	YES	YES	NO
E2EE 1-1 & Group Chats (default)	YES	YES	YES	YES	YES
E2EE Video Calls	YES	YES	YES	YES	YES
No Personal/Business Phone number or email registration	YES	NO	YES	YES	YES
Onion Routing or IP address masking	YES	NO	NO	YES	YES
Decentralized servers	YES	NO	NO	YES	YES
Non-Attributed external phone number & calling	YES	NO	NO	NO	NO
Decentralized VPN	YES	NO	NO	NO	NO
Federation (all APP users can communicate across enterprise)	YES	N/A	NO	YES	YES
File Sharing (up to 5G), w/low to high side (classified) capability	YES	NO	NO	NO	NO
Secure Cloud Large File Sharing	YES	NO	NO	NO	NO
Private Enclave: Secure Cloud Server dedicated to organization (optional)	YES	NO	NO	NO	NO
Secure Containers or “Virtual” Phones	YES	NO	NO	NO	NO
Disables AdTech or location Tracking	YES	NO	NO	NO	NO
Admin/Device Mgmt. Console	YES	NO	YES	YES	YES
Organizationally Managed Teams	YES	NO	NO	YES	YES
Dedicated 24/7-365 support	YES	NO	N/A	YES	YES

See other case studies and learn more about the SIP Program here:
https://www.SecurityExecutiveCouncil.com/about/solution_innovations.html