BABYLON

SECURE SMARTPHONES SYSTEM

HighSecLabs
Highest Security Solutions

THE CHALLENGE

- In recent years, the mobile network has become the highest-quality communications network, widely used throughout the world, enabling the transmission of voice and data at the highest quality and speed.
- The integration of the smartphone into the advanced mobile networks has made us all captive users. This wide usage also includes security organizations and government officials who need to keep their information classified.
- As a result, the use of offensive cyber tools has greatly increased, making them a significant threat to anyone using a smartphone. Information collected on the smartphones gives the attacker a significant advantage, either operationally or as leverage for extortion.
- The wide use of smartphones by national security and other government and military personnel together with their email and social network access, created a major global security vulnerability.

The architecture of the system we have developed, integrated and tested with our customers enables to secure the use of the most advanced smartphone. This system supports operation security up to the level of Top-Secret / National Security. This solution is called BABYLON.

CURRENTLY AVAILABLE SOLUTIONS

Existing solution	Security impact
• Organizations prohibit the use of cellular phones to specific users / in specific environments.	• Either user will use cellular devices without permission or will suffer from bad communications.
• Organizations allow Bring Your Own Device (BYOD) for limited on-job use.	• Users will use their devices while violating security rules. Wide classified information leakages.
• Organizations using software enhanced secure smartphones.	• These smartphones are easily targeted and hacked by cyber offensive tools.
• Organizations developing custom high-security smartphones with strong hardware encryptions.	• Products become obsolete before they are deployed.
• Organizations ignoring the issue.	• Wide violations of information security guidelines.

OUR SOLUTION

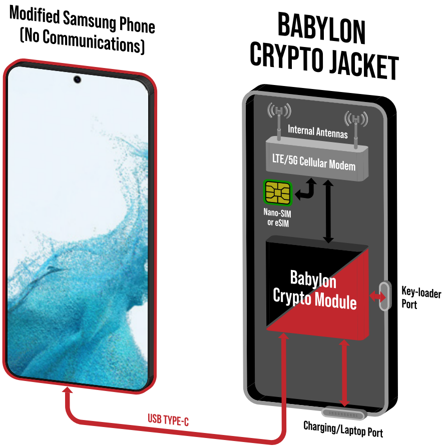
- Babylon is a relatively new concept that converts the latest commercially available smartphones into a top-secret military devices. A device that can still communicate with other devices on any commercial cellular network.
- Unlike other solutions existing in the market, Babylon does not rely on software encryption. It uses an external mobility hardware encryption module. The smartphone is highly modified by HSL to disable all other wireless interfaces.
- Babylon provides a wide range of standard Android applications – not only secure calls.

Babylon is a truly Ultra-secure communication solution that cannot be hacked by any existing Cyber Offensive tool or Spyware.

- Babylon is an end-to-end solution for governments, defense, and commercial organizations that want to enable efficient and secure mobile and home communications.

REVOLUTIONARY ARCHITECTURE

- Samsung's latest Android smartphone has been modified by HSL to remove all external wireless communication features.
- Smartphone loaded with customized ROM to assure secure boot and Data At Rest encryption.
- The slim Babylon jacket is attached to the modified smartphone and connected through the USB Type-C interface.
- The jacket contains the Babylon hardware encryption module which creates an encrypted tunnel to the organization's red (classified) servers.
- The jacket also contains an independent cellular modem that enables data communications on any commercial cellular network.
- Unlike other ultra-secure phones, Babylon does not mix Red and Black domains in one device. The phone is 100% red domain and only a small portion of the jacket is a Black domain.



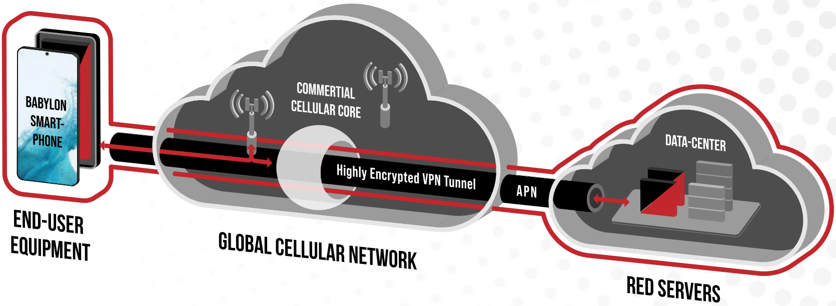
- Babylon hardware encryption is designed as an NSA Type-1 device with military security strength.
- Babylon encrypted tunnel is capable of withstanding attacks from organizations, countries, and even superpowers.
- Babylon jacket enables physical key-loading through the key-loader port. Keys are safely protected in a hardware safe.

SUPERIOR SECURITY

- Babylon jacket features a military-strength hardware encryption module.
- Babylon module uses multiple highly-isolated cores to protect from network attacks both from the Red and from the Black domains.
- Networks at both sides are equally protected by configurable state-full deep packet inspection firewalls running on dedicated network processors.
- Security monitoring services run constantly to detect potential physical or network penetration attempts.
- Babylon crypto module design features the industry's largest set of tampering protection and detection. The jacket is equipped with battery-backed anti-tampering sensors as well as erase push-button to zero the device.
- Babylon jacket uses a military key-loader to load keys. Keys are quickly rotated during device operation.
- Babylon smartphone does not support cellular calls – all calls are VoIP. All data communications are tunneled to the customer classified data-center.

HSL SECURE MOBILITY SYSTEM – CELLULAR INFRASTRUCTURE

- Babylon smartphones are connected to one or more customer data-centers.
- Connection is made using a highly-protected VPN tunnel.
- Commercial cellular operator network core connected to the customer data-center via APN (Access Point Name).
- Babylon creates a virtual high-security network inside any public cellular network.
- Data-center is having one or more crypto gates, HSM, and red network servers.
- Red network servers run required red applications such as voice/video conference, PTT, email, messaging, etc.



COMPATIBILITY

- The use of the latest Samsung commercial smartphones enables the use of standard commercial software applications widely available for Android platforms.
- In most cases, customers do not need to develop complex tailored applications. No special software drivers are required to operate and manage Babylon devices.
- Users can connect an auxiliary tethered device such as a classified laptop or other network devices to access classified networks remotely.

Babylon is essentially an end-to-end solution for conducting highly secure communications over the infrastructure of commercial mobile operators.

- Babylon smartphone is easy to use and intuitive to the end-user. Basic training is needed to most users.

ADVANCED MANAGEMENT SOLUTIONS

Babylon crypto jackets can be managed locally or remotely through a secure web-based user interface stored on the red processor. It has an extensive, customizable set of features that can be configured from any connected device with the appropriate permissions and a web browser. Additional tools for managing the jacket are available through the Android widget, Windows application, and Linux service. All firmware and software components of the jacket can be managed locally or remotely via the secure Firmware Over-The-Air feature.

SYSTEM FEATURES – HIGH LEVEL

- All communications pass through strong encryption hardware. Calls are VoIP.
- Agnostic to the cellular network. Works worldwide (in roaming).
- Encryption can be customized from commercially available AES-256 to NSA Type-1 equivalent. Products can be supplied without encryption (“Crypto-Ready”).
- Babylon User Equipment (UE) is isolated from the world and the Internet. It is connected only to the red Babylon Core network.
- Babylon Core can be located on the customer's premises or the cloud (Amazon, Google, or in other cloud services).
- Babylon red core is a well-protected, classified IT environment. However, it may have secured interfaces to other services/networks.
- Babylon requires isolated red applications. It does not have access to the Internet.

HIGH SEC LABS

IS A CYBER SECURITY COMPANY FOCUSING ON CYBER DEFENSE FOR NATIONAL SECURITY INFRASTRUCTURE.

www.highseclabs.com

Patents: www.highseclabs.com/patents/. HLT28371 Rev 1.1