BABYLON

SECURE SMARTPHONE SYSTEM

HighSecLabs
Highest Security Solutions

THE CHALLENGE

- The mobile network has become an indispensable communications network, used worldwide, transmitting voice, video and data at the highest quality and speed.
- The integration of the smartphone into advanced mobile networks has made us all captive users. Users now include security organizations and government officials who must protect their classified information.
- 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 a 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, has created a major global security vulnerability.

The architecture of the system we have developed, integrated and tested with our customers provides secure 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 prohibiting the use of cellular phones to specific users / in specific environments.	• The user either uses cellular devices against policy or will suffer from tedious and inconvenient communications.
• Organizations allowing Bring Your Own Device (BYOD) for limited on-job use.	• Users will use their devices while violating security rules. Wide potential for classified information leakages.
• Organizations using software enhanced secure smartphones.	• These smartphones are easily targeted and hacked by offensive cyber tools.
• Organizations developing custom high-security smartphones with strong hardware encryptions.	• Products become obsolete before they are even deployed.
• Organizations ignoring the issue.	• Wide violations of information security guidelines.

THE BABYLON SOLUTION

- Babylon is an innovative concept that transforms the latest commercially available smartphones into top-secret military grade devices, while still being capable of communicating over any commercial cellular network with other devices.
- Unlike other solutions existing in the market, Babylon does not rely on software encryption. It uses a built-in mobility hardware encryption module. The smartphone is 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 true ultra-secure communication solution that cannot be hacked by any existing offensive cyber tool or spyware.

- Babylon is an end-to-end solution for governments, defense, and commercial organizations requiring efficient and secure mobile communications.

REVOLUTIONARY ARCHITECTURE

- Samsung's latest Android smartphone has been modified by HSL to remove all external wireless communication features.
- The smartphone is loaded with a customized ROM, assuring 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 that creates an encrypted tunnel to the organization's Red (classified) servers.
- The jacket also contains an independent cellular modem for 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 Black domain.

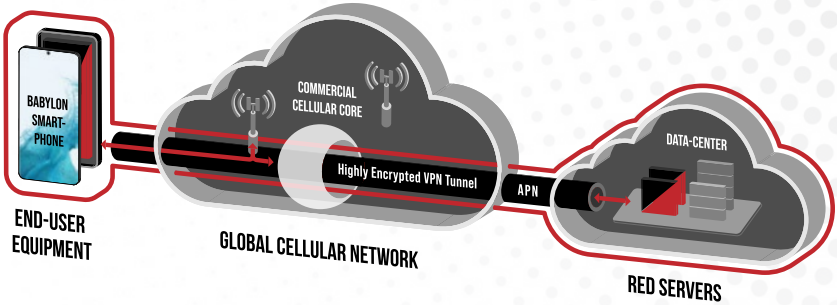
- Babylon hardware encryption is designed as an NSA Type-1 device with military security strength.
- The Babylon encrypted tunnel is capable of withstanding attacks from organizations, countries, and even superpowers.
- Babylon supports physical key-loading through the key-loader port. Keys are safely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

SUPERIOR SECURITY

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

HSL SECURE MOBILITY SYSTEM – CELLULAR INFRASTRUCTURE

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



COMPATIBILITY

- Using the latest Samsung commercial smartphone facilitates 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 to Babylon such as a classified laptop or other network devices to access classified networks remotely over a hardware secured tunnel.

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

- The Babylon smartphone is easy to use and intuitive to the end-user. Only basic training is needed by most users.

ADVANCED MANAGEMENT SOLUTIONS

The Babylon crypto jacket 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 an Android widget, a Windows application, and a 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 voice and video over IP.
- Works with all cellular networks worldwide.
- Encryption can be customized from commercially available AES-256 to NSA Type-1 equivalent. Products can be supplied without encryption (“Crypto-Ready”).
- The Babylon smartphone is isolated from the world and the Internet. It is connected only to the Red Babylon Core network.
- The Babylon Core can be located on the customer's premises or in the cloud (Amazon, Google, or other cloud services).
- The 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 open Internet.

HIGH SEC LABS

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

www.highseclabs.com

 HLT28371 Rev 1.3