

# **Keeps Your Calls Confidential**





#### Secure

end-to-end encrypted calls

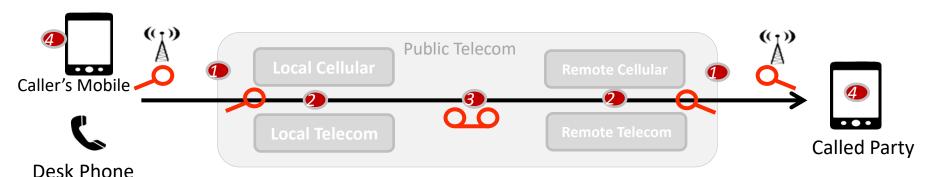
between

mobiles and desk phones

over any

wired & wireless 3G/4G/WiFi networks seamlessly

# User's call vulnerability



Once device is registered, it's unique hardware ID (IMEI) and network SIM ID (IMSI) are logged by the local visited network or by unauthorized hackers, which can track the user's location history.

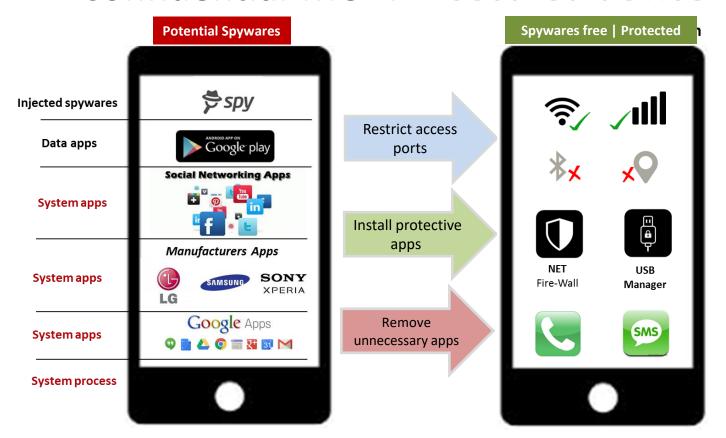
**Call's info of Caller/Called ID are logged** by all networks on the call path, including foreign networks. Unauthorized entities can monitor the online call records with their own tools for reveal ing valuable confidential personal/business connections.

Call conversation can be eavesdropped/recorded by authorized governmental agencies and by unauthorized abusive entities. Call eavesdropping can reveal the most intimate calls and most commercial valuable info.

Spywares are malicious apps which can silently eavesdrop all calls.

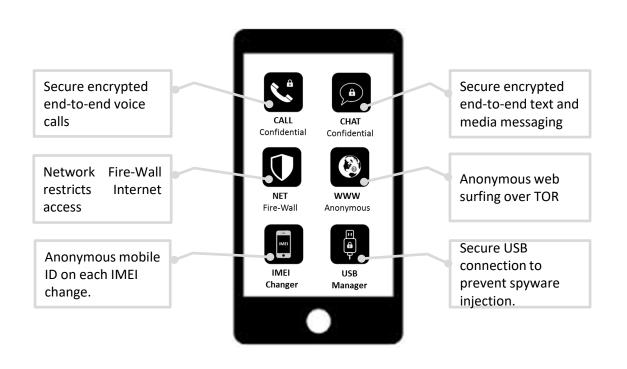
Most spywares are injected via innocent app installed by the device's owner.

## **Confidential-MOBILE** secured device





# **Confidential-MOBILE**Secure Dedicate Mobile Device





# **Confidential-CALL** app

End-to-End Secure Encrypted Call

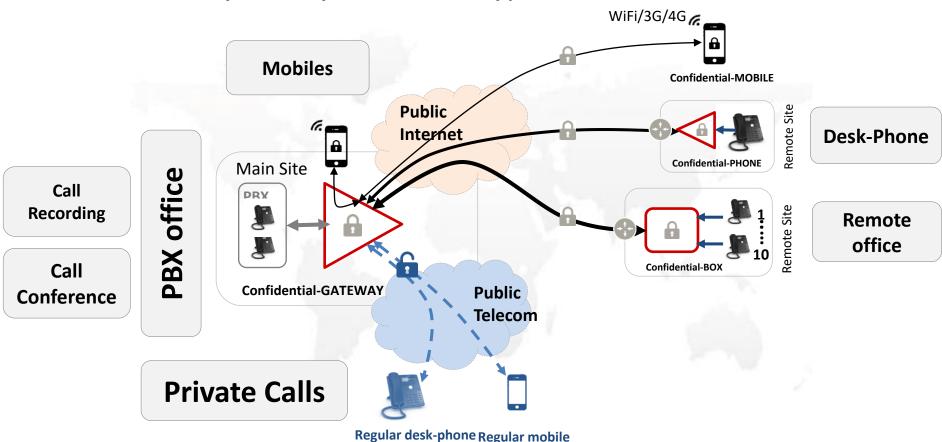


- ♠ Secure encrypted end-to-end phone calls.
- ♠ Strong fresh unbreakable encryption key per each call initiation
- A Protected from call parties identification.
- Protected from call tracking.
- Protected from call eavesdropping.



#### **Confidential-GATEWAY** server

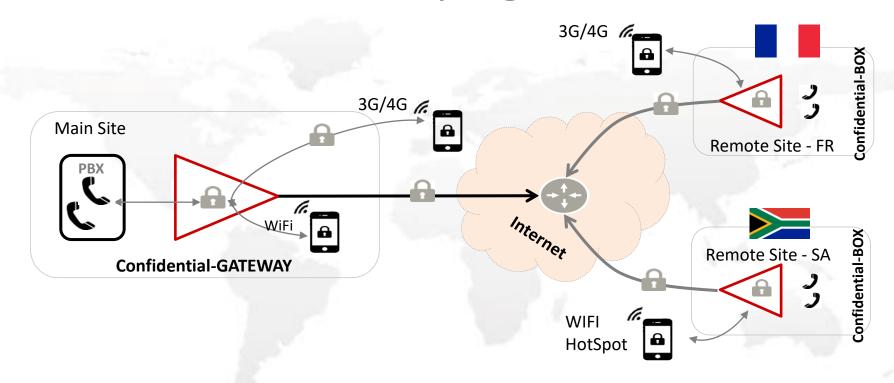
Any-to-Any Secure Encrypted End-to-End Calls





## **Confidential-GATEWAY**

# Secure multiple global sites



**Ministry of Foreign Affairs** 

**Remote International Embassies** 

### U2 Global Marketing