HighSecLabs
Highest Security Solutions Ltd.

HSL PHONE IMPLANT FOR DIGITAL / VOIP PHONE PROTECTION

Exclusively control and isolate all phone microphones and speakers to prevent eavesdropping and air-gapping of isolated computers. HSL Phone Implant blocks all phone's audio capabilities while not in a legitimate phone conversation.

Phones are everywhere - even in the most classified offices and meeting rooms.
Compromised phones may be exploited to eavesdrop conversations taking place at the vicinity of the phone.

Compromised phones can intercept/generate covert audio signals to communicate with air-gapped computers in order to breach isolated networks.

Protect against eavesdropping

SECURITY FEATURES:

- **Designed to meet special customer needs:**
  - The implant's hardware is custom designed to fit with the customer's specific phone models.
  - Implant settings are adjustable by a software configuration tool.
- **Securely installed by a trusted authority:**
  - The implant is installed by HSL in a secure assembly line.
- **Prevent reception and transmission of audio originated by the phone's malicious hardware or firmware:**
  - The implant exclusively controls and isolates all phone microphones and speakers.
  - The implant is a hardware barrier that physically separates the speakers and microphones wiring from the phone's motherboard.
  - Regardless of the phone firmware or hardware settings, microphones and speakers operate only as pre-determined by the implant settings, defined by the customer.
- **Hardware Anti-Tampering:**
  - Any attempt to open the phone's enclosure will activate an anti-tamper system making the product inoperable.
  - Blinking LEDs provide a clear indication of a tampering event.
  - Special holographic tampering evident labels on the product's enclosure provide a clear visual indication if the product has been opened or compromised.

WHAT MAKES A PHONE A SECURITY THREAT?

- **Phones run all-purpose computer hardware:**
  - Phones are vulnerable to computer attacks as they run all-purpose computer hardware and have limited (if any) hardware and software protection.
- **Untrusted Firmware:**
  - There is no way to ensure that there are no "back doors" in the phone's firmware. Phones are designed by companies that cooperate with the NSA.
  - The phone's built-in firmware upgrade mechanism can be exploited to stealthily load hostile firmware and gain complete remote control of the phone.
- **Untrusted Hardware and Supply Chain:**
  - Phones are designed by companies that collaborate with the NSA.
  - Phones are manufactured by companies directly related to the Chinese government.
  - There is no way to ensure that the phone was not compromised at any phase of the supply chain.
- **High Quality Audio:**
  - A modern phone is built and designed to enable excellent audio quality and therefore can easily eavesdrop to conversations in a nearby room separated by a drywall.

OPERATIONAL HIGHLIGHTS

- **Maintain security without compromising usability:**
  - The implant has no negative effect on performance or user experience.
  - One simple rule for using the phone – take the handset off the hook– that's it! (also, while listening to a phone conversation through the phone's speaker).

- **Audio and visual notifications provide clear and simple user indications of the phone's secure state.**
  - Once secured with HSL Phone Implant the phone provides the user with a clear audio and visual indication of its security status.
  - Green LED is ON = Phone is Secure = You can speak freely in the room without fear of eavesdropping.
  - Red LED is ON = Phone's audio is active = Do not conduct classified conversations in the vicinity of the phone.
  - Audio warnings (beeps) & Phone LEDs are flashing = Phone is Secure yet the implant detected that the handset is off hook while there is no active phone conversation.

SUPPORTED PHONE MODELS

MODEL	MANUFACTURER	P/N	
CP-8851 2nd Gen	CISCO	CPN13221	
CP-8851 3rd Gen	CISCO	CPN23853	
CP-7821 / 41	CISCO	CPN16207	
CP-8865	CISCO	CPN16653	
440HD	AUDIOCODES	CPN70464	
CORAL 281S	TADIRAN	CPN15698	
LIP-9030	LG	CPN17372	
T-58	YEALINK	CPN70872	
J179	AVAYA	CPN70931	

Protect against air-gap breaching