

HSL SECURITY SOLUTION FOR **VoIP Telephony Endpoints**



VoIP Telephony as a major security threat

1

VoIP Phones Protection

- VoIP phones are everywhere - even in the most classified offices and meeting rooms.
- Large deployment = large potential attack surface.
- Last older PSTN phones in service are being replaced by modern IP telephony.
- New IP Telephony brings many value added features including Video Conferencing, phone directory, and smart caller ID functions.

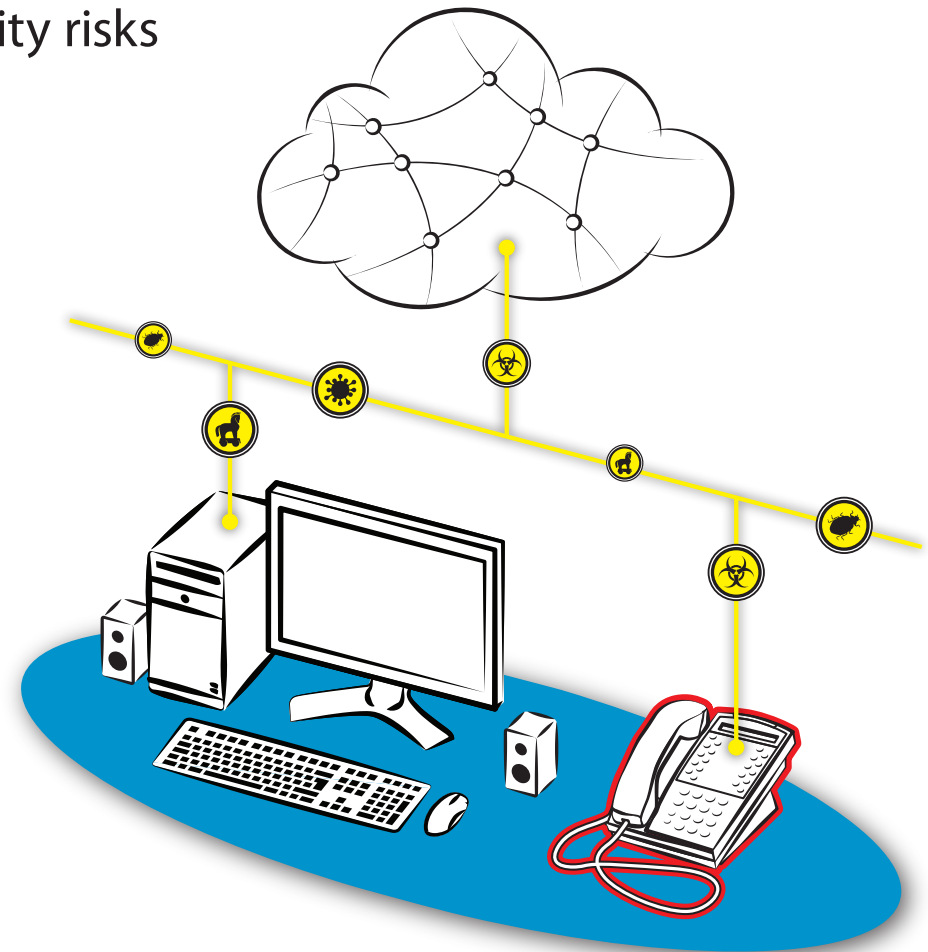


VoIP Telephony as a major security threat

2

VoIP Phones Protection

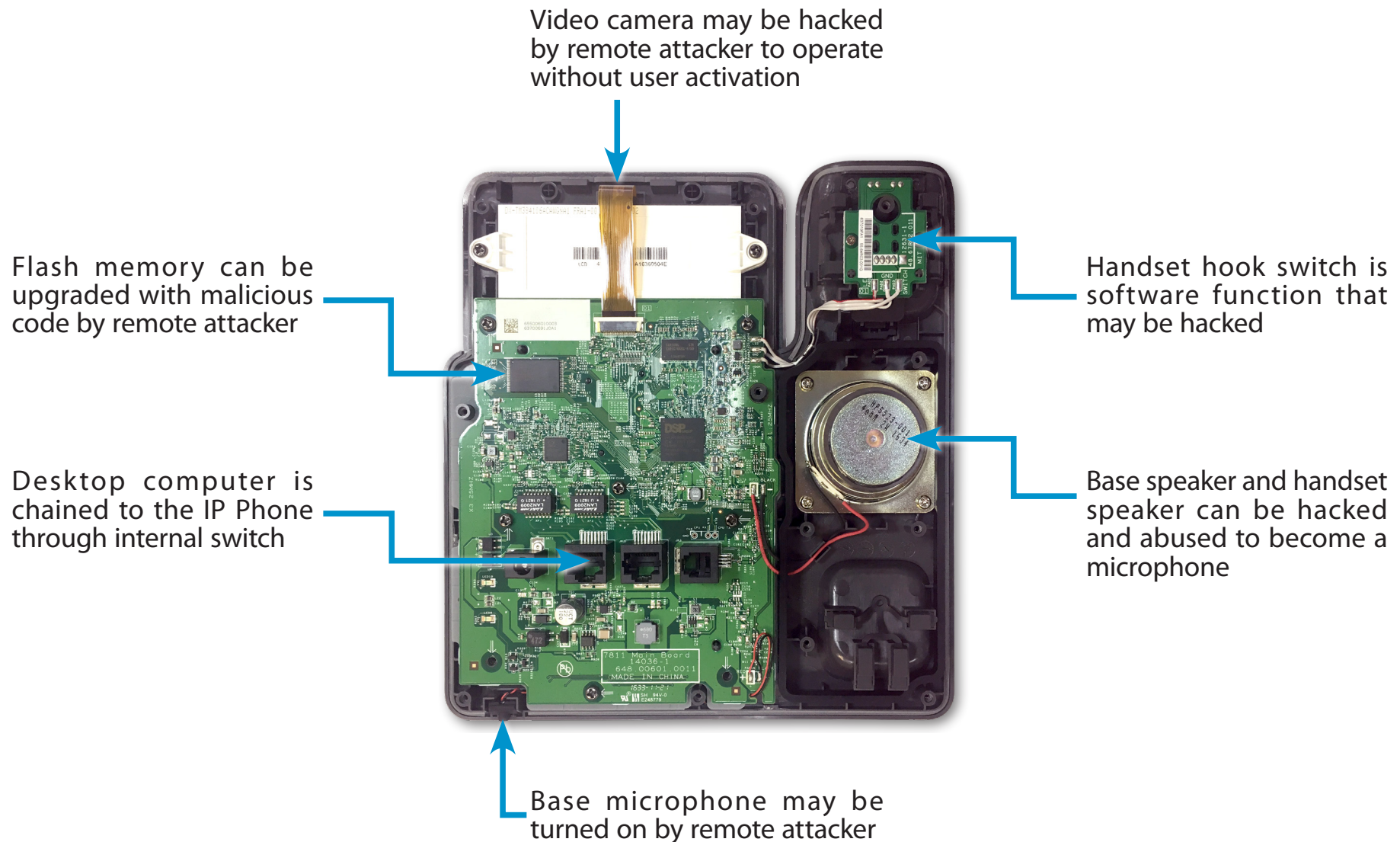
- Many organizations are not aware of the security risks involved with VoIP deployments.
- VoIP phones are NOT perceived as a security threat although being exposed to the outside world through networks that have internet access.
- VoIP telephony offers great opportunity for external attackers to launch audio eavesdropping or undetected video surveillance.
- VoIP telephony supply chain is typically high risk.



VoIP Telephony as a major security threat

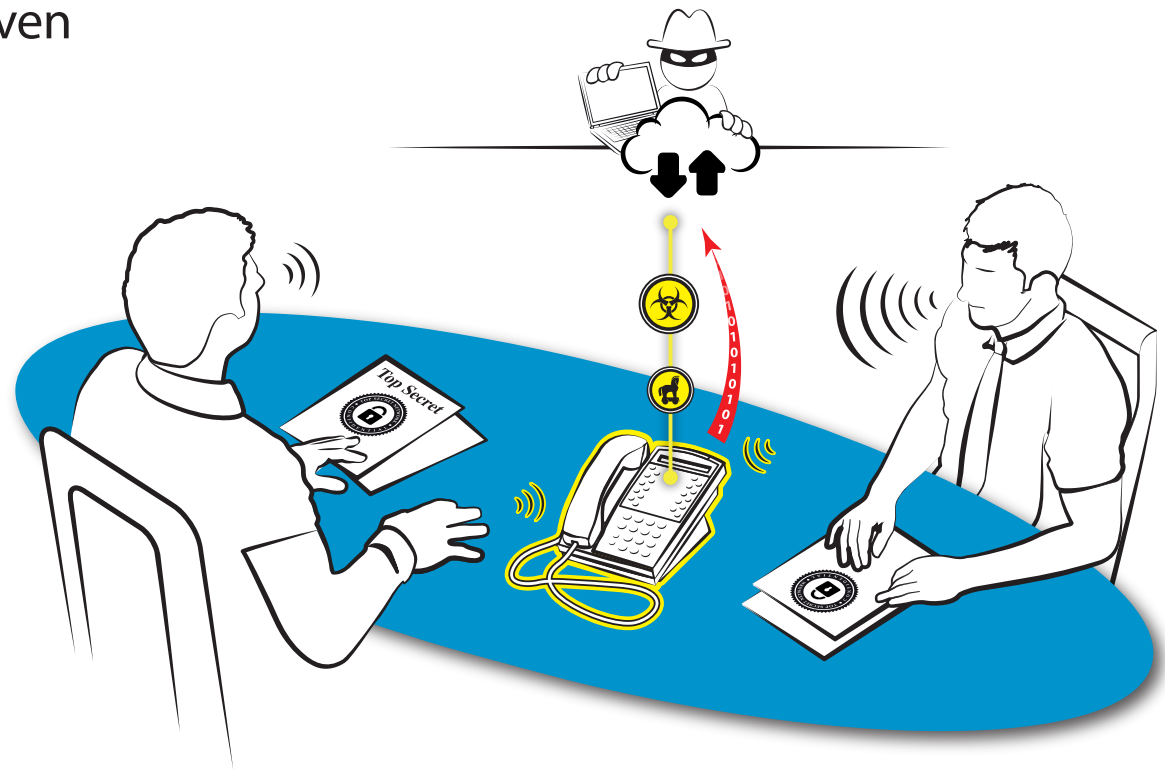
3

VoIP Phones Protection

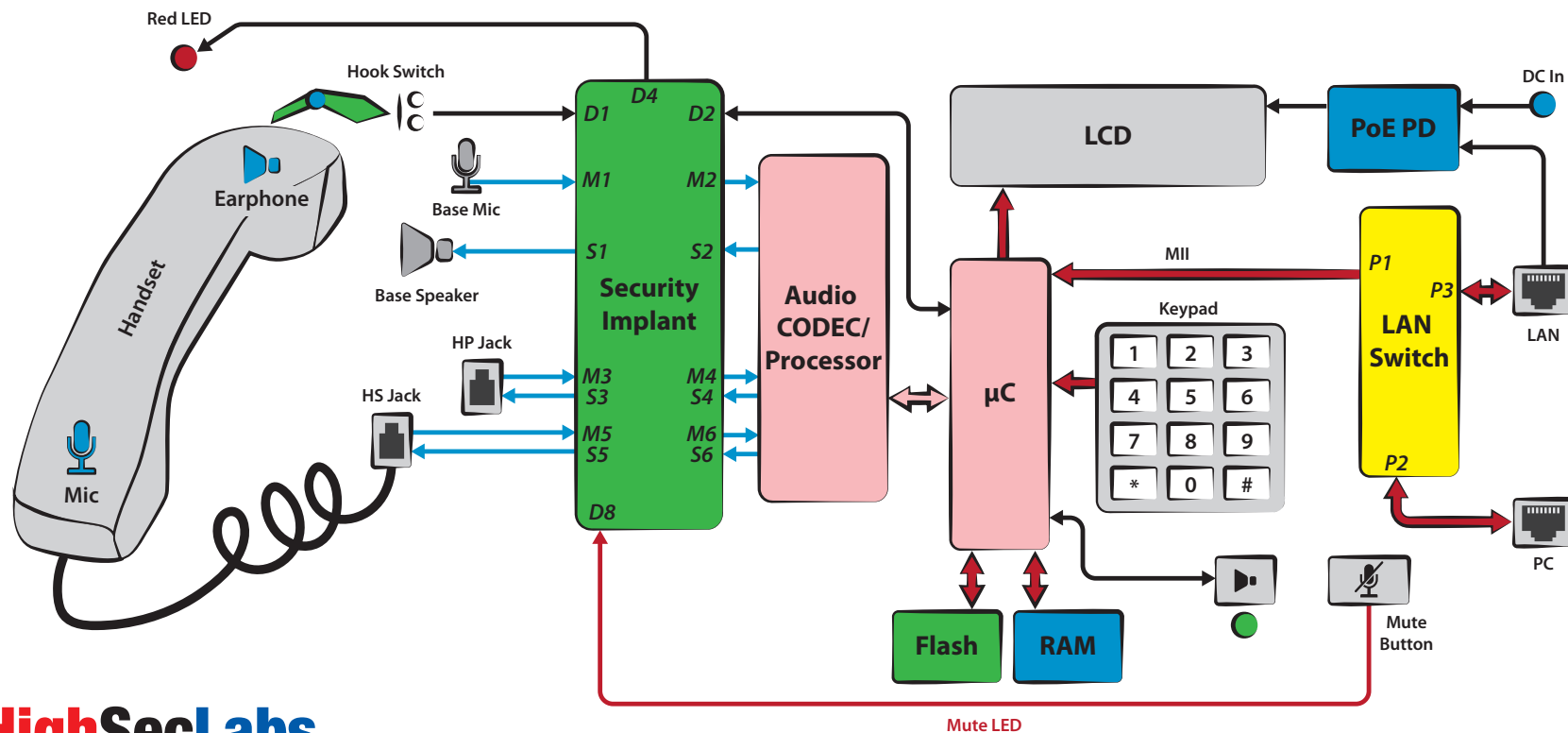


Eavesdropping through a hacked IP Phone

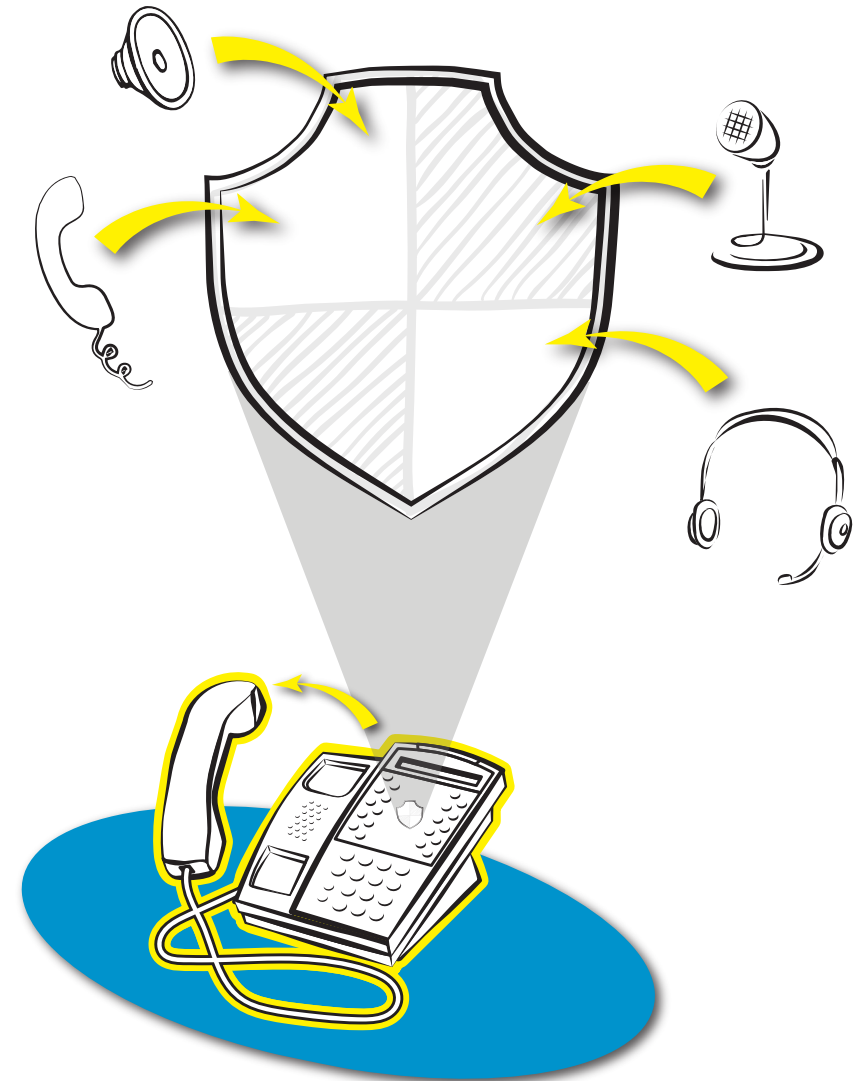
- Any IP Phone can be easily converted into a surveillance audio bug using malicious software.
- Remote attacker may eavesdrop on private/classified conversation or even open the device video camera.
- Most commercial IP Phones are lacking basic security functionality of modern network devices.
- VoIP Phones may be used to breach air gap to deliver information or malicious code to/from classified computers having speakers / microphone.



- HSL Security enhanced IP Phone is modified to include a trusted security implant.
- HSL Security implant is positioned between the phone and all of the acoustic peripherals, blocking it unless the user provides a positive and distinctive action.
- Security enhanced IP Phone provides clear user indications when the phone is in secure state or when it is sensing its environment (active).

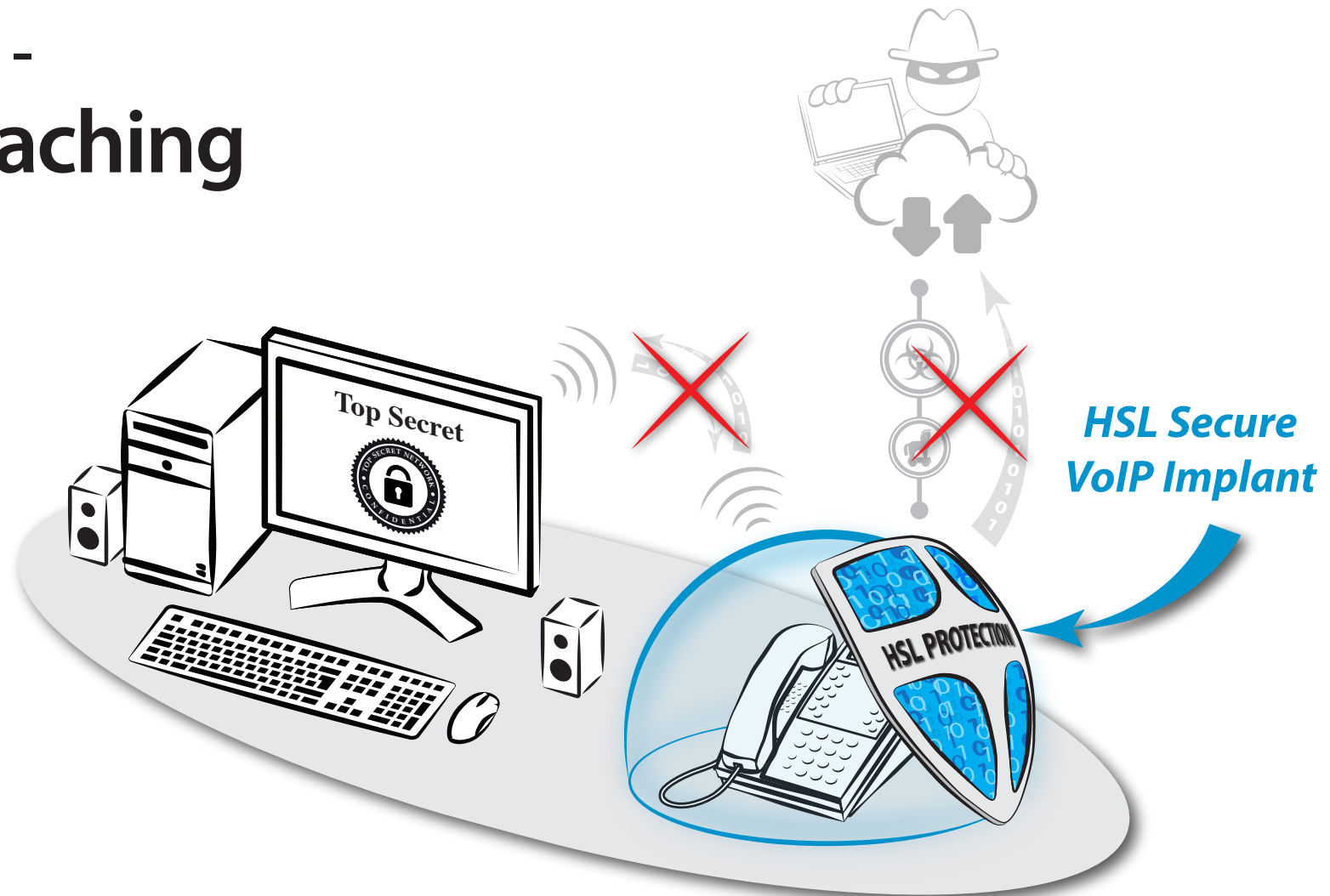


- HSL's Security enhanced IP Phone Implant will only allow access to the phone acoustic peripherals once the user physically lift the handset.
- No reliance on phone software or hardware.
- Base Speaker and headset calls are possible but only when the handset is lifted.
- The implant allows normal phone operation without any negative effect on performance or user experience.
- Audio and visual notifications provide clear and simple user indications of the phone's secure state.



Protect against - Air-gap breaching

- Phone will not receive audible or ultrasonic audio signals from nearby computer.
- External IP Phones may be securely placed and used in classified zones.



Supported Phone Models

8

VoIP Phones Protection

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	





THANK YOU!