

# VoIP Security Management Threat Detection and Control

Peter Cox  
CEO  
UM Labs Ltd  
peter@um-labs.com

September 2009

## Agenda

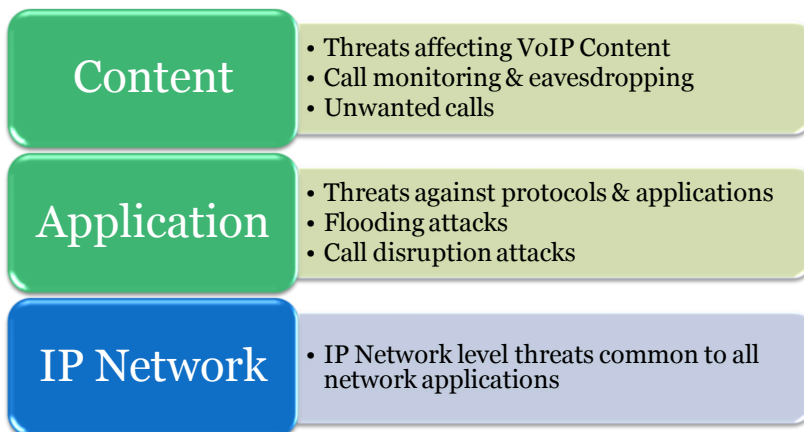
- About the speaker
- Categorising VoIP Security Threats
- Potential Threat Impact
- Threat Detection and Control
- VoIP Security Audits

## Peter Cox

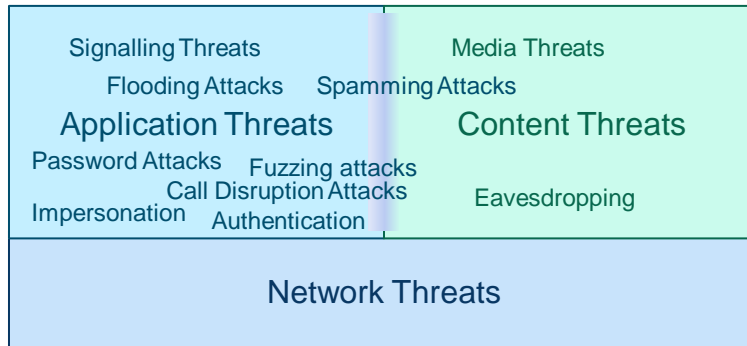
- Founder and CEO of UM Labs Ltd
  - Developer of VoIP Security and encryption products
  - Regular speaker on VoIP Security Topics
  - In-depth VoIP Security Workshops
- Co-founder of Borderware Technologies Inc
- 25 Years experience in Internet protocols and security



## VoIP Threat Taxonomy



## VoIP Threat Classification



## SIP Signalling Threats

- SIP Signalling Threats arise from
  - Misuse of the SIP Signalling
  - Lack of comprehensive authentication
  - SIP Design, Network Architecture and deployment (NAT Challenges)
- Threats associated with every SIP method



## SIP Methods (1)

SIP Method	Function	Threats
REGISTER	Identify a phone to a PBX	Register flooding Deregistration Authentication Flooding Password attacks
INVITE	Place a call	Call Flooding Call Hijacking
BYE	Terminate a call	Call Termination attack
OPTIONS	Determine status of a device	Information Discovery
SUBSCRIBE	Request Presence Information	Information Discovery
NOTIFY	Send Presence Information	Information Discovery Flooding



## SIP Methods (2)

SIP Method	Function	Threats
MESSAGE	Send Instant Message	Flooding Content Threats
REFER	Transfer or re-direct a call	Call Hijacking
CANCEL	Cancel a call (before its answered)	Call Termination attack
ACK	Acknowledge a previous message	Dependent on previous message
PUBLISH	“Event State Publication” (Presence information)	Not yet widely implemented



## REGISTER Request

```
REGISTER sip:voipcode.org SIP/2.0
Via: SIP/2.0/UDP 192.168.19.12:5060;branch=z9hG4bK1d1bc13a8c075154cde
Max-Forwards: 70
To: <sip:fred@voipcode.org>
From: <sip:fred@voipcode.org>;tag=1916793
Call-ID: SL-tpucghjy-41543ff7@192.168.19.12
CSeq: 10131 REGISTER
Expires: 3600
Allow: INVITE, ACK, CANCEL, OPTIONS, BYE, REFER
Contact: <sip:fred@192.168.19.12>
User-Agent: SIP Library: Unix V1.1 Build: May 14 2007, 17:44:30
Content-Length: 0
```



## PBX Processing

- On receiving a REGISTER request a PBX must
  - Check the domain
  - Lookup the user
  - Send an authentication challenge if needed
  - Process an authentication response



## Registration Floods

- Easy to generate floods of registration messages
- No knowledge of target (other than network address) needed

```
REGISTER sip:fake.org SIP/2.0
Via: SIP/2.0/UDP 172.16.60.2:5060;branch=z9hG4bK2ab423c10ac18124cd
Max-Forwards: 70
To: <sip:user181@fake.org>
From: <sip:user181@fake.org>;tag=2817299
Call-ID: SL-mcekflpr-262d41de@172.16.60.2
CSeq: 769 REGISTER
Expires: 600
Allow: INVITE, ACK, CANCEL, OPTIONS, BYE, REFER
Contact: <sip:user181@172.16.60.2>
User-Agent: SIP Register Flood Test
Content-Length: 0
```



## Summary: Registration Attacks

Attack	Potential Impact	Prior Knowledge Required	Ease of Exploit 1 (complex) – 10 (trivial)
Registration Flood	Very High (can lead to system failure)	Non (other than identify of target)	10
Registration Authentication Flood	Very High (can lead to system failure)	Non (other than identify of target)	10
De-registration Attack	High (disrupts service to targeted phones)	Phone identify (name/number and domain)	9
Password dictionary attack	High (circumvents authentication)	Packet capture	5

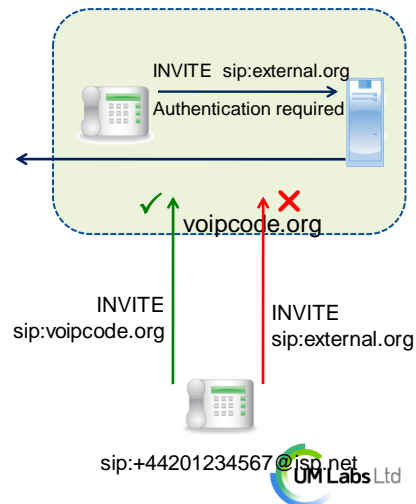
## SIP Invite

- INVITE sets up a call between two (or more) SIP phones
- Optionally authenticates the calling phone
- INVITE requests can originate from anywhere
- Many attack options



## INVITE Authentication Limitations

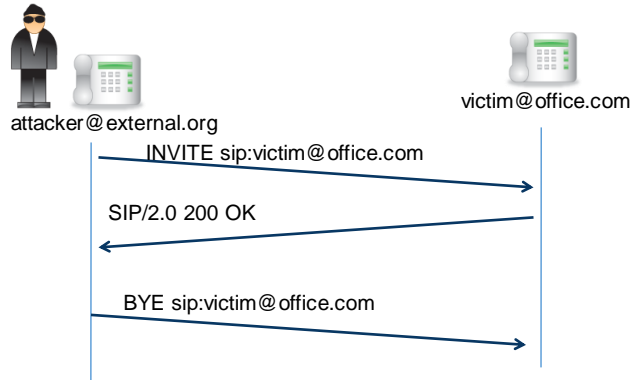
- INVITE authentication can be applied **ONLY** to...
  - Calls originating from a local domain
    - To a phone in a local domain
    - To an external domain
    - To a gateway (SIP Trunk, PSTN etc)
- Calls from an external domain cannot be authenticated
  - Destination of calls from external domains *should* be limited to a local domain
- Analogous to the email open relay problem, but with financial penalties



## Simple Call Flood

```
./sipinvite -f attacker@external.org -t victim@office.com
           -d 0 -v pbx.office.com
```

Place a call and hang-up after 0 seconds



## Summary: INVITE Attacks

Attack	Potential Impact	Prior Knowledge Required	Ease of Exploit 1 (complex) – 10 (trivial)
Call flooding	Very High (can lead to system failure)	Non (other than identify of target)	10
VoIP Spam	High (can delay important calls and will lead to user dissatisfaction)	Phone identify (name/number and domain)	10
Call Hijack	Very High (can re-direct calls)	Active call parameters (needs live network monitoring)	4

## Summary: BYE Attacks

Attack	Potential Impact	Prior Knowledge Required	Ease of Exploit 1 (complex) – 10 (trivial)
Call Termination	High (will disrupt calls to targeted phones)	Active call parameters (needs live network monitoring)	6



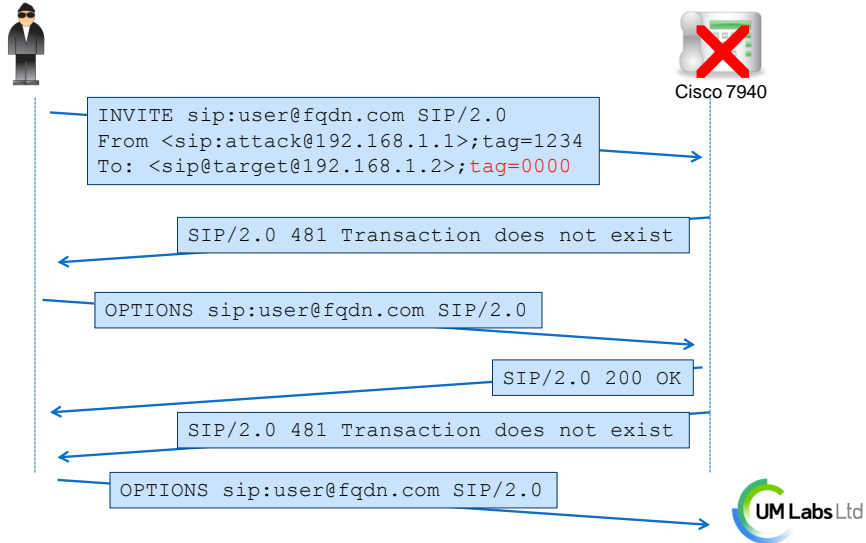
## Multiple Message Threats

- Some known threats require multiple Sip methods
- Messages are valid, or have only minor errors
- Tend to be product specific
- Two examples:
  - SIP Remote DoS on Cisco 7940 Phone
  - Grandstream GXV3000 Remote Eavesdropping Vulnerability

[http://voipsa.org/pipermail/voipsec\\_voipsa.org/2007-August/002422.html](http://voipsa.org/pipermail/voipsec_voipsa.org/2007-August/002422.html)



## SIP Remote DoS on Cisco 7940



## SIP Remote Eavesdropping on Grandstream GXV3000

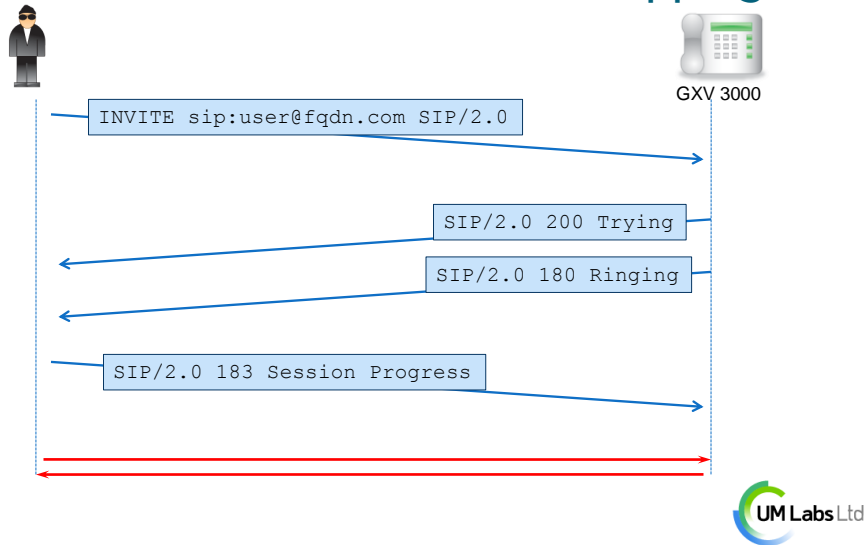
### GXV3000 IP Video Phone

The GXV3000 is an easy and affordable way of communicating face-to-face over any distance. It is ideal for any multi-media communication environment, the virtual office and all IP video communications for business or residential users.

The GXV is an advanced IP video phone based on SIP and H.264/H.263 standard, competitively priced and easy to use. The GXV combines sleek design and technology features with excellent picture quality, ease of deployment and broad interoperability with 3rd party SIP products. The GXV-3000 is the first H.264 IP video phone that supports real-time high-quality video at bandwidths as low as 32kbps and up to 1Mbps. The phone allows nearly all viewing angles via its 5.6 inch TFT adjustable LCD screen and VGA camera, enabling high-quality videoconferences from your home or office.



## Grandstream Remote Eavesdropping



## Grandstream Remote Eavesdropping

- All messages are valid
- 183 Call progress is out of normal sequence
- Phone does not ring, goes silently off-hook
- Effectively becomes a bugging device
- Phone stays off-hook until its re-set
  - DoS Attack as a side-effect
  - Other Grandstream phones partly susceptible

## Threat Summary - Multiple SIP Methods

Threat	Traffic Monitoring Required?	Blocked by Firewalls?	Impact	Ease of Exploit
Multiple Message Attacks	No	No	10	8

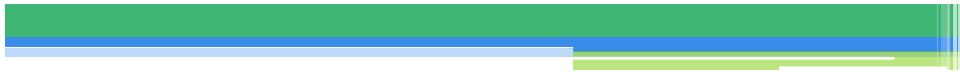
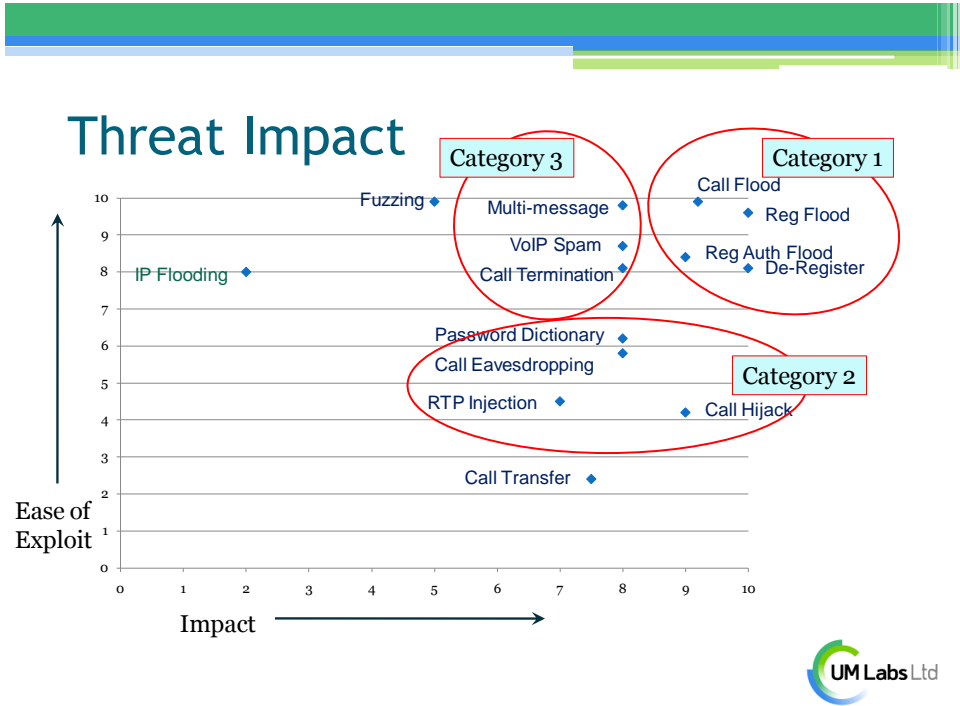
- Examples were
  - Cisco 7940 Remote DoS
  - Grandstream Remote Eavesdropping



## Threat Summary - Media

Threat	Traffic Monitoring Required?	Blocked by Firewalls?	Impact	Ease of Exploit
Call Eavesdropping	Yes	No	8	6
RTP Injection (and variants)	Yes	No	7	5





## Categorising Threats

Threats dependent on Network Monitoring	Password Dictionary Call Termination Call Hijacking Call Eavesdropping RTP Injection	Category 1 Category 2 Category 3
Threats requiring some prior knowledge of target network	Authentication Flood De-Registration VoIP Spam Multiple Message Threats	Category 1 Category 3
No Preconditions*	Malformed Messages Register Flood Call Flood	Category 1

\* With the exception of knowing the identity of the target



## Detecting Attacks

### Easy to detect attacks

- Registration flooding
- Call flooding
- Call Termination attacks
- Denial of service attacks
- RTP Injection attacks

### Stealth attacks

- Call eavesdropping
- Toll fraud (until you get the bill)

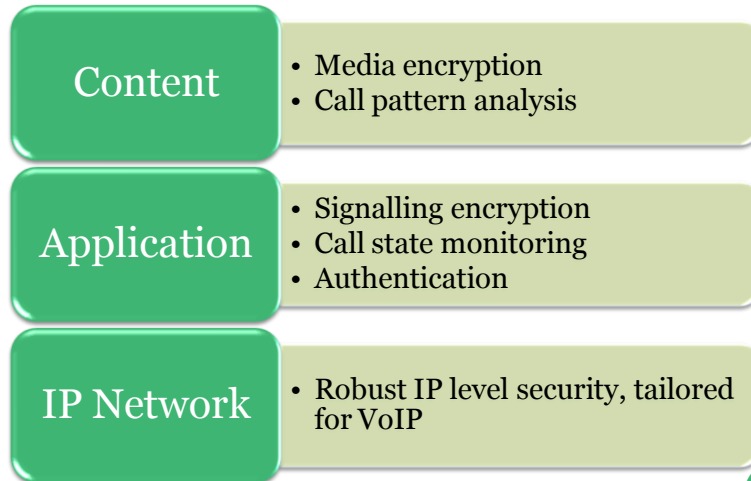


## Countering the threats

- Countering VoIP threats requires specialist security controls
  - Complexity of VoIP applications and protocols
  - Impact of identified threats
  - Broad scope of applications
- These controls are beyond the scope of standard security products (firewalls)
- Controls require a specialist security gateway



## Designing a VoIP Security Gateway

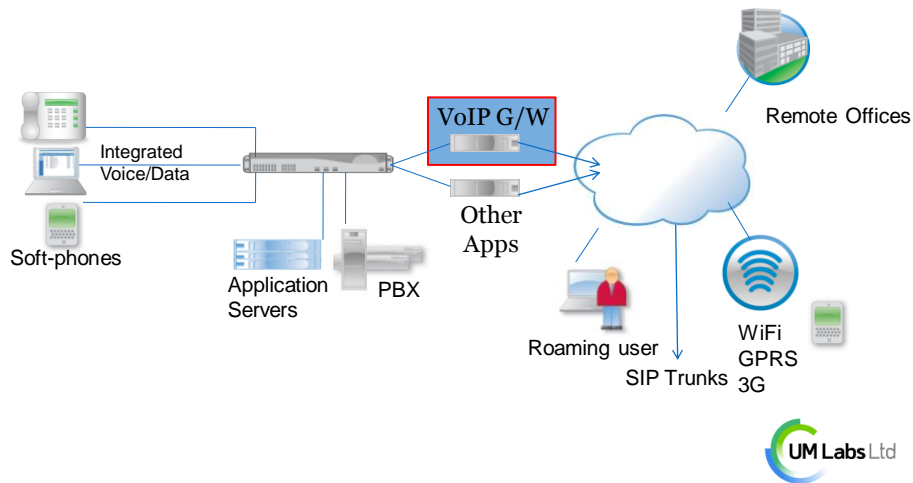


## Media and Signalling Encryption Options

- **SDES/SRTP**
  - Built in as standard
  - Secures calls to remote users and “private trunks”
  - Supported by hardware phones (e.g. snom) and softphones (e.g. Counterpath)
- **ZRTP**
  - Designed by Phil Zimmermann
  - Secures calls to remote users
  - Key exchange over media stream
  - Supported for softphones and on a wide range of cell phones



## Deploying VoIP Security



## Security Audits and threat detection, the bad news....

- There are no easy solutions
- Standard tools, ISS, Nessus and others useful for detecting IP level threats
  - Should always be part of a VoIP Security audit
- Don't rely solely on IP level tools
- Don't expect logs to show all attacks

## Nessus Scan of an IP-PBX

Nessus Scan Report  
-----

### SUMMARY

- Number of hosts which were alive during the test : 1
- Number of security holes found : 0
- Number of security warnings found : 3
- Number of security notes found : 21

- Target system had a number of serious vulnerabilities including:
  - Call Hijacking, Eavesdropping, Call flooding
  - Failed 37% of RFC 4475 Malformed message tests
  - Limitation on REGISTRATION rate



## Auditing a VoIP Network

### Standard Tools & Techniques

- Port Scans
- Vulnerability scans
- Patch management
- VoIP Aware Firewalls
- Log Analysis
- Target all points of the infrastructure
  - IP-PBX
  - Phones
  - Gateways

### Specialist Tools & Techniques

- Protocol specific testing
  - Torture Tests
  - Protocol conformance
- Flooding Tests
  - Registration Flooding
  - Call flooding
- Authentication tests
  - Directory Harvest attacks
  - Password dictionary attacks
- Hijacking and Eavesdropping tests



## VoIP Security Audits

- Effective Audits require specialist tools combined with *ad-hoc* techniques and low-level analysis
- Example, analysis of Unistim (Nortel CS1000 proprietary VoIP Protocol)

The screenshot shows a Wireshark capture of network traffic. The packet list pane displays several packets, including Telnet and Unistim traffic. The Unistim packets show payload sequences of 0xFFFFFFFF and 0x4E906620, along with NAK and Hello (state Standby) messages.

No.	Time	Source	Destination	Protocol	Info
7	11:23:17.006012	192.168.19.45	192.168.19.18	TELNET	TELNET Data ...
8	11:23:17.069165	192.168.19.18	192.168.19.45	TELNET	TELNET Data ...
9	11:23:17.072546	10.8.120.42	10.8.49.4	UNISTIM	Payload seq - 0xFFFFFFFF
10	11:23:17.072924	10.8.49.4	10.8.120.42	UNISTIM	NAK For seq - 0x4E906620
11	11:23:17.074615	10.8.120.42	10.8.49.4	UNISTIM	Payload seq - 0xFFFFFFFF
12	11:23:17.074809	10.8.49.4	10.8.120.42	UNISTIM	NAK For seq - 0x4E906620
13	11:23:17.076543	10.8.96.3	224.0.0.2	HSRP	Hello (state Standby)
14	11:23:17.076598	10.8.120.42	10.8.49.4	UNISTIM	Payload seq - 0xFFFFFFFF
15	11:23:17.076790	10.8.49.4	10.8.120.42	UNISTIM	NAK For seq - 0x4E906620
16	11:23:17.078556	10.8.120.42	10.8.49.4	UNISTIM	Payload seq - 0xFFFFFFFF
17	11:23:17.078748	10.8.49.4	10.8.120.42	UNISTIM	NAK For seq - 0x4E906620
18	11:23:17.080483	10.8.120.42	10.8.49.4	UNISTIM	Payload seq - 0xFFFFFFFF
19	11:23:17.080673	10.8.49.4	10.8.120.42	UNISTIM	NAK For seq - 0x4E906620
20	11:23:17.081113	192.168.19.18	192.168.19.45	TELNET	TELNET Data ...

## Unistim Vulnerability Analysis (1)

- Unistim is a very low level protocol
- Event Messages sent between phone and PBX
  - '9' key pressed (phone -> PBX)
  - Turn on message LED (PBX -> phone)
- Each Message ACK'ed

<b>Phone</b>	<b>CS1000</b>
UNISTIM Msg Seq: 001 →	
UNISTIM Msg Seq: 002 →	
	← UNISTIM ACK: 002
	← UNISTIM Msg Seq: 1234
UNISTIM ACK: 1234 →	

- A reserved ACK (FFFFFFFF) resets message sequence

## Unistim Vulnerability Analysis (2)

- Low level analysis showed that:
  - Messages are not authenticated by PBX or phone
  - Messages use UDP, easy to spoof source IP
  - Messages may easily be injected to both phones and PBX
- Threats:
  - Phones loose service when flooded with Unistim messages
  - Phones loose service when flooded with any traffic (e.g. badly configured syslog feed)
  - Calls can be established, re-routed, terminated by sending spoofed Unistim messages to PBX



## About UM Labs

- Products
  - EC4200 and RC2100 SIP Security Controllers
  - SIP Security Gateways ranging from small office to large enterprise
- Consultancy and Training
  - VoIP and UM Security Audits
  - Security Workshops
- Contact
  - Phone: +44 20 3021 3200
  - VoIP: sip:info@um-labs.com
  - Email: info@um-labs.com
  - Web: www.um-labs.com

