

VoIP Forensics

Vasilis Katos

Democritus University of Thrace, Greece

The team

- × **Lilian Mitrou,**
 - + University of The Aegean
 - + Athens University of Economics and Business
- × **Ioannis Psaroudakis,**
 - + Democritus Univ. of Thrace

Metadata...



- ✘ “Time stamp”
(carbon dating)
- ✘ “author”
(anthropology)
- ✘ Geo Location
(...geographic location)

a few thousand years later...

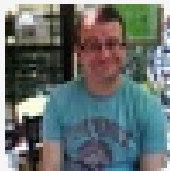
Monitoring (a.k.a. surveillance)



Legislation

- ✘ EU Directive 2006/24/EC
 - + Data Retention Directive
 - + “Serious Crime”
- ✘ What data?
 - + Traffic and location data
 - + Unsuccessful call attempts
 - + *NO* content
- ✘ Who shall retain the data?
 - + ISPs, telecoms, ...?

Impact



Scott Thompson @ScozzaThompson

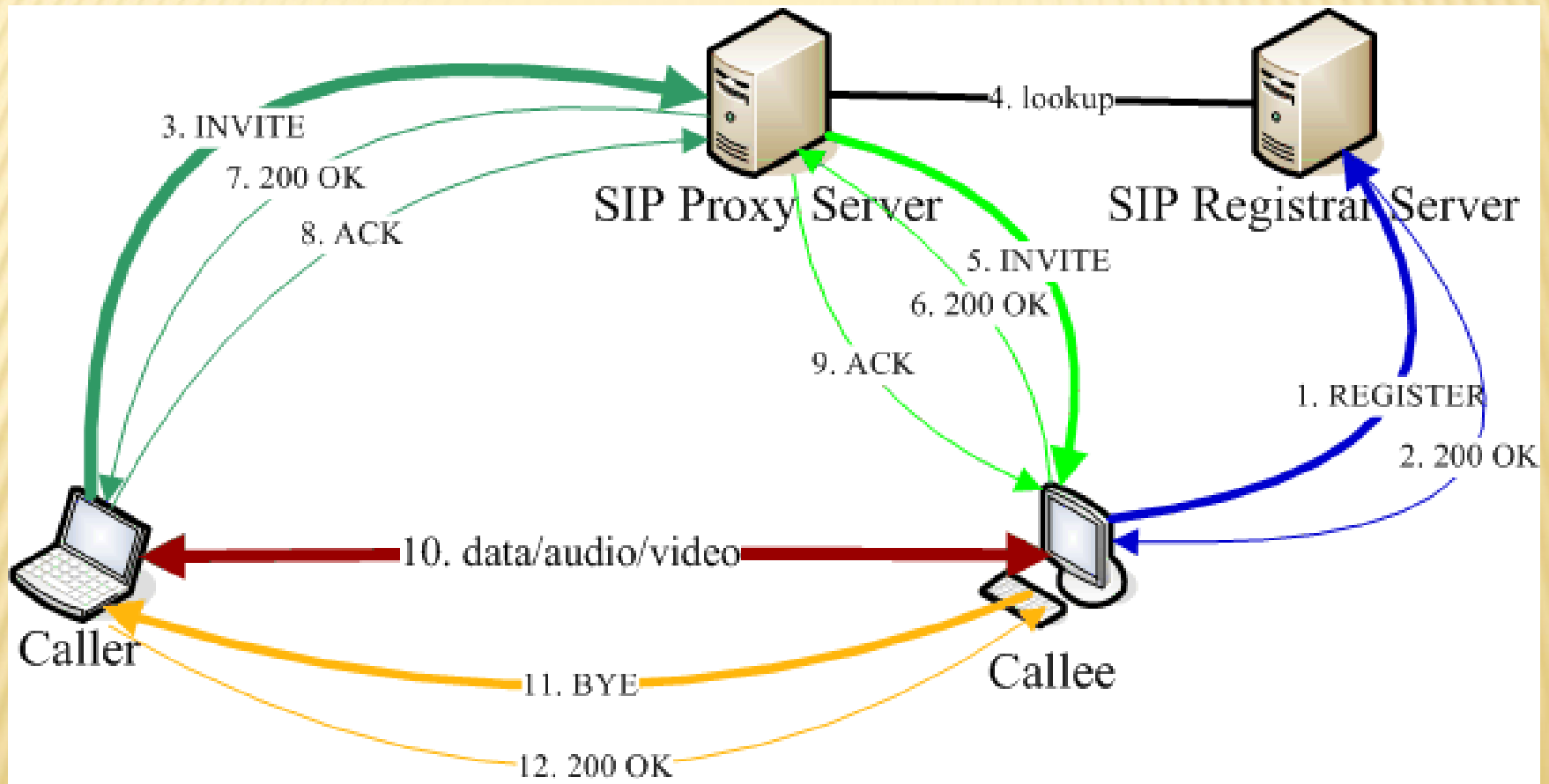
30 Oct

#PaymentsConf13 factoid of the day, more people own a mobile than a toothbrush.

Expand

← Reply ↻ Retweet ★ Favorite ⋮ More

Session Initiation Protocol (SIP)



SIP Header

1/2

Time 2013-05-01 23:35:57.978170

Internet Protocol Version 4, Src: 5.54.64.210 (5.54.64.210), Dst:
192.xxx.xxx.37 (192.xxx.xxx.37)

Session Initiation Protocol

Request-Line: INVITE sip:71150@sip.duth.gr SIP/2.0

Message Header

Via: SIP/2.0/UDP 5.54.64.210:61624;branch=z9hG4bK-d8754z-320fc157e67ba641-1---d8754z-;rport

Contact: <sip:402@5.54.64.210:61624>

To: "71150" <sip:71150@sip.duth.gr>

From: "jpsaroud windows" <sip:402@sip.xxxx.gr>;tag=3f498445

Call-ID: MmFmYWFjNTk1ZTQzOTdhM2JiODJiINDAYZGNkOTRiZmU.

CSeq: 1 INVITE

User-Agent: **eyeBeam release 1102q stamp 51814**

Session Description Protocol

Owner/Creator, Session Id (o): - 5 2 IN IP4 5.54.64.210

SIP Header

2/2

Owner Network Type: IN

Owner Address Type: IP4

Owner Address: 5.54.64.210

Session Name (s): **CounterPath eyeBeam 1.5**

Connection Information (c): IN IP4 5.54.64.210

Connection Network Type: IN

Connection Address Type: IP4

Connection Address: 5.54.64.210

Media Attribute (a): alt:1 4 : UhYE2Wox sLbn3kLo 5.54.64.210 24784

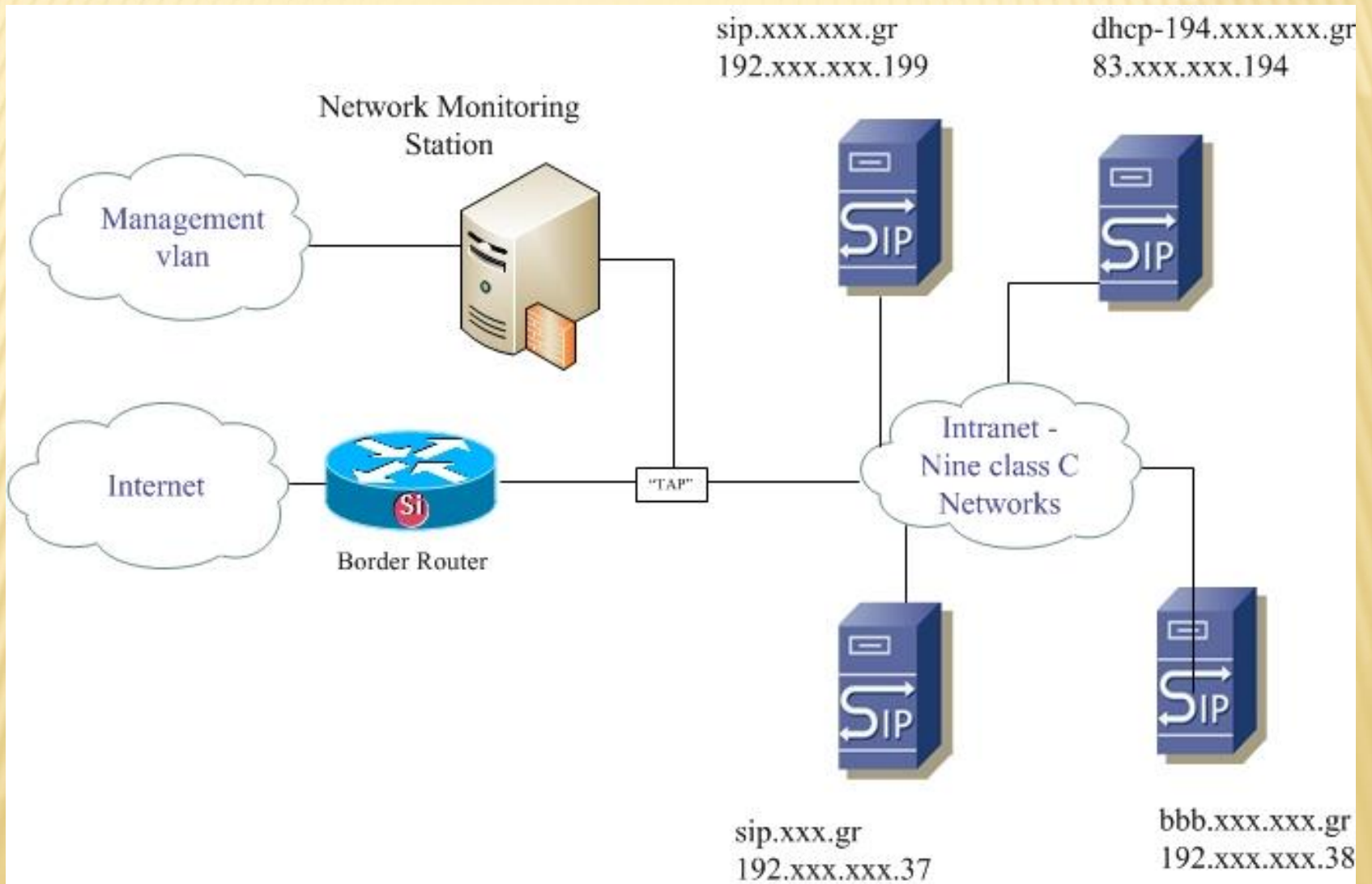
Media Attribute (a): alt:2 3 : R828U4V/ IW4gLyQM **10.10.10.1** 24784

Media Attribute (a): alt:3 2 : M4f701Fm 5Gw9wOoX **192.168.61.1**
24784

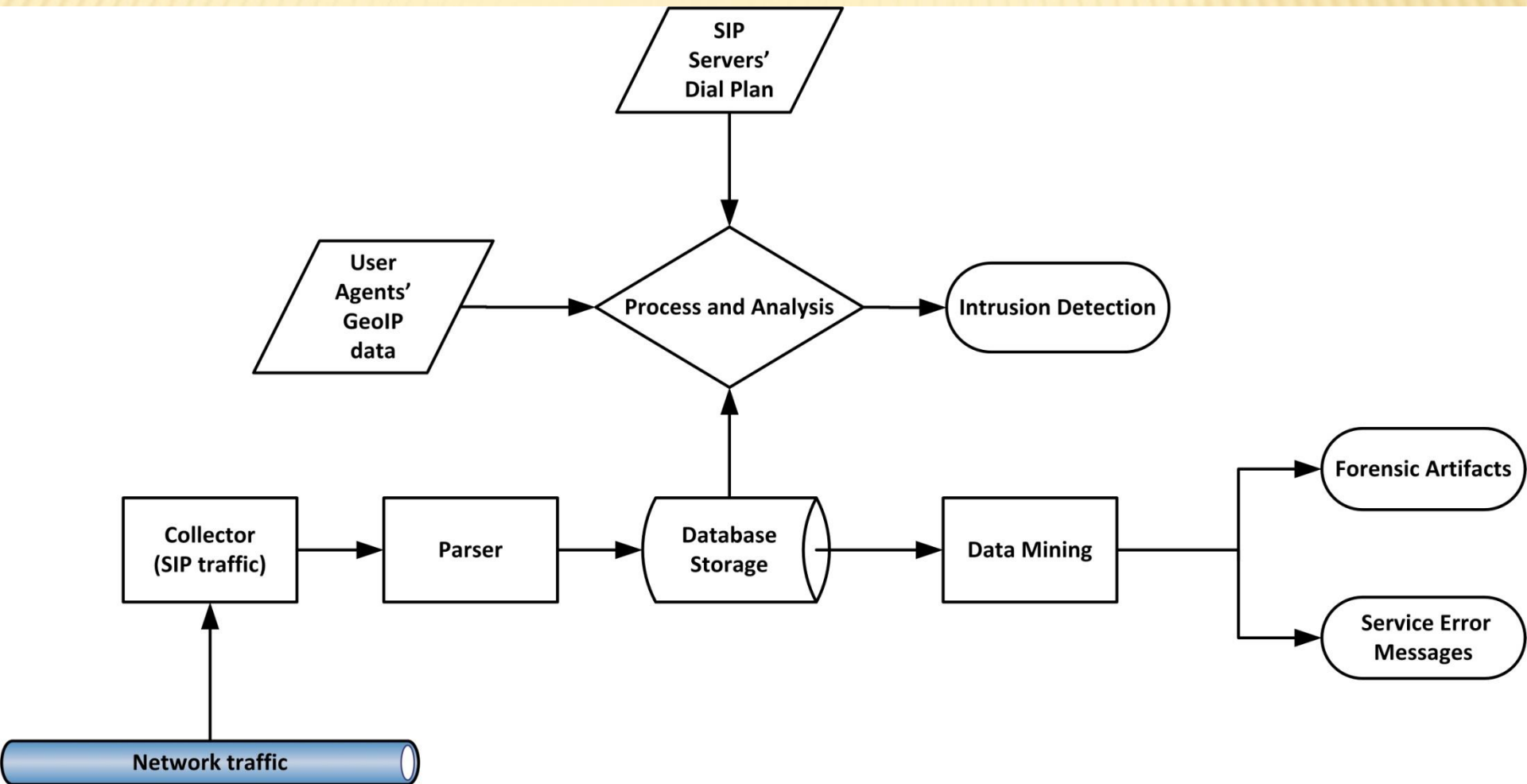
Media Attribute (a): alt:4 1 : BndXE2LR CPxnl5x9 **192.168.111.1**
24784

Info: Request: INVITE sip:71150@sip.xxxx.gr, with session description

The testbed



The analysis framework



Legitimate User – user agent string

Number of SIP messages	Value	Artifact	Authenticated User
772	3CXPhone for iPhone 1.1.5	3CX Softphone for Iphone or Ipad	604@sip.xxx.xxx.gr
2164	Acrobits SIPIS (http://www.acrobits.cz)	Softphone for Devices	e51@83.xxx.xxx.194
30	Acrobits Softphone/5.3.2	Softphone for Devices. Version 5.3.2 is for Iphone or Ipad.	e51@83.xxx.xxx.194
13949	C470IP/022270000000	Siemens Gigaset IP phone model C470	ssip@83.xxx.xxx.194 sp1@83.xxx.xxx.194
4739	C610 IP/42.050.00.000.000	Siemens Gigaset IP phone model C470	lin@83.xxx.xxx.194
215	CSipSimple_GT-I9100-15/r1916	SipSimple softphone for Android running in Samsung I9100 Galaxy S II smartphone.	756@sip.xxx.gr
3319	Intracom/Intracom-1.63.A	Netfaster IAD router 1.63 firmware with SIP Analog Telephone Adaptor	402@sip.xxx.gr

Legitimate User – register process

Timestamp	Source IP	User Agent SIP	ContactNumber of SIP messages
3/13/13 8:23	X9.210.204.5X	3CXPhone for iPhone 1.1.5	<sip:401@192.168.2.102:5065>
3/12/13 22:57	X9.210.21.3X	3CXPhone for iPhone 1.1.5	<sip:401@192.168.2.101:5065>
3/15/13 22:13	X4.225.194.9X	Acrobits Softphone/5.3.2	<sip:e51@192.168.0.128:5090>
3/11/13 8:45	X4.225.194.9X	C470IP/022270000000	<sip:ssip@192.168.0.2:5060>
3/15/13 0:05	X4.68.112.21X	C470IP/022270000000	<sip:mam@192.168.1.72:5062>
3/11/13 8:43	X4.68.71.1X	C470IP/022270000000	<sip:mam@192.168.1.72:5062>
3/17/13 17:03	X6.12.185.16X	CSipSimple_GT-I9100-15/r1916	<sip:756@X6.12.185.16X:5060;> <sip:756@192.168.0.125:5060>

Legitimate User – INVITE request in media SDP attributes

Timestamp	Source IP	User Agent	SDP Connection Info	SDP Media Attributes
3/11/13 16:33	X9.210.182.12X	3CXPhone for iPhone 1.1.5	192.168.2.101	rtcp:4001 IN IP4 192.168.2.101
1/5/13 23:35	X3.212.132.15X	eyeBeam release 1102q stamp 51814	X3.212.132.15X	Media Attribute (a): alt:1 4 : UhYE2Wox sLbn3kLo 5.54.64.210 24784 Media Attribute (a): alt:2 3 : R828U4V/ IW4gLyQM 10.10.10.1 24784 Media Attribute (a): alt:3 2 : M4f701Fm 5Gw9wOoX 192.168.61.1 24784 Media Attribute (a): alt:4 1 : BndXE2LR CPxnI5x9 192.168.111.1 24784
3/15/13 9:37	X4.65.125.23X	Telephone 1.0.4	192.168.178.22	rtcp:4001 IN IP4 192.168.178.22

Private LAN disclosure from SIP messages

Apple iPad or iPhone
with 3CXPhone 1.1.5 SIP User Agent
Dynamic IPs: 192.168.2.102
at May 1 2013 23:32



Android Motorola Atrix with
CSipSimple r1916 SIP User Agent
Dynamic IPs: 192.168.2.103
at May 1 2013 23:32



INTERNET
through HOL ISP

Intracom Netfaster IAD
1.63 WLAN
with public IP: 5.54.64.210
at May 1 2013 23:30



Private LAN



Linux PC
with Ekiga 3.2.6 SIP User Agent
Dynamic IPs: 192.168.2.107
at May 1 2013 23:32



MS Windows PC
with eyeBeam release 1102 SIP User
Agent
Static IPs: 192.168.2.50
10.10.10.1
192.168.111.1
192.168.61.1
at May 1 2013 23:35

Malicious or non legitimate users

✘ SipVicious

- + User-agent: "friendly-scanner", OPTIONS

 - [sip:100@8x.xxx.xxx.23](tel:sip:100@8x.xxx.xxx.23)

 - + INVITE [sip:5221@192.xxx.xxx.38](tel:sip:5221@192.xxx.xxx.38)

✘ SipCli

- + INVITE sip:0972592646879@192.xxx.xxx.38

- + Private IP from SDP owner header

✘ "excessive spoofing"

- + User-agent: OcaXowTU4mYZ2m9

Legitimate users

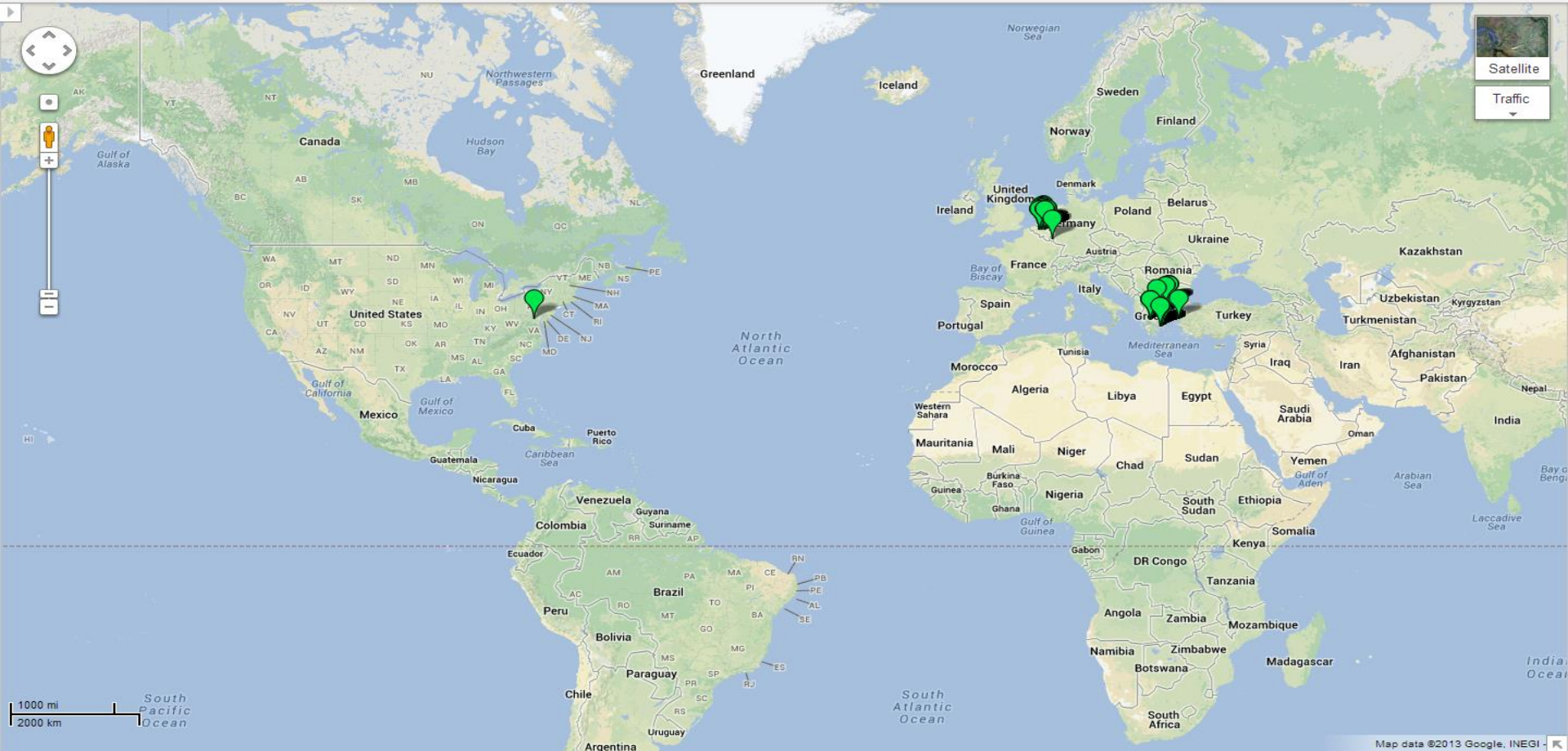
+Ioannis Search Images **Maps** Play YouTube News Gmail Drive Calendar More -

Google

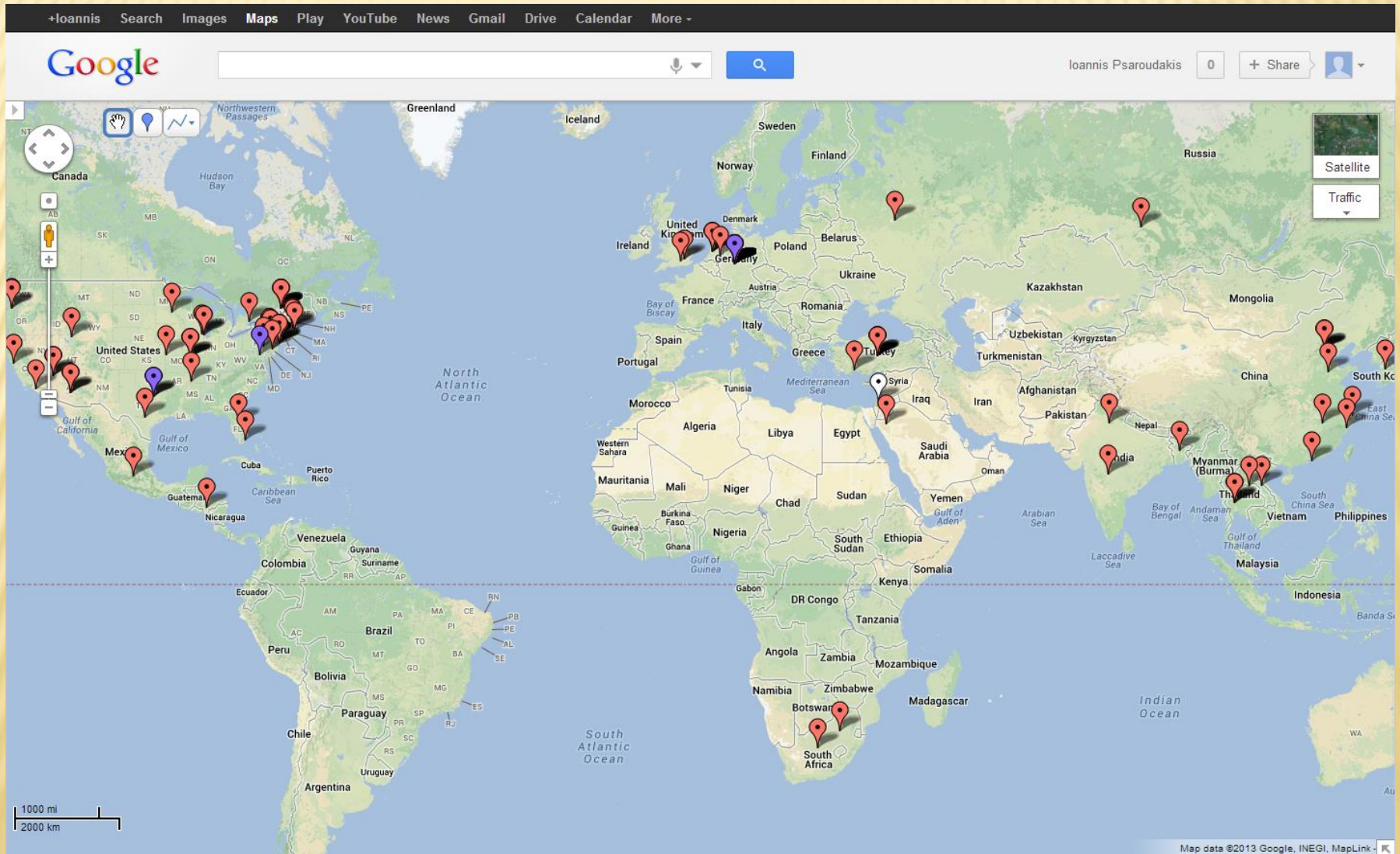


Ioannis Psaroudakis 0

+ Share



Malicious users



Conclusions

- ✘ A wealth of volatile traffic data can be used for identifying entities participating in VoIP communication
 - + Forensic readiness
- ✘ Data retention scope?
- ✘ Applications result to increased complexity
 - + The “CEO golf effect”
 - + Information leaks?

References

1. Bo-Lin W., "A study on the forensic mechanisms of VoIP attacks: Analysis and digital evidence", *Digital Investigation*, vol. 8, no. 1, pp. 56-67, 2011.
2. Dritsas, S., Tsoumas, B., Dritsou, V., Konstantopoulos, P., Gritzalis, D., "OntoSPIT: SPIT Management through Ontologies", *Computer Communications*, vol. 32, no. 2, pp. 203-212, 2009.
3. François, J., State, R., Engel, T., Festor, O., "Digital forensics in VoIP networks", in *Proc. of the IEEE International Workshop on Information Forensics and Security*, pp. 1-6, 2010.
4. Gritzalis, D., Katos, V., Katsaros, P., Soupionis, Y., Psaroudakis, J., Mentis, A., "The Sphinx enigma in critical VoIP infrastructures: Human or botnet?", in *Proc. of the 4th International Conference on Information, Intelligence, Systems and Applications*, IEEE Press, 2013.
5. Gritzalis, D., Marias, G., Rebahi, Y., Soupionis, Y., Ehlert, S., "SPIDER: A platform for managing SIP-based spam over Internet Telephony", *Journal of Computer Security*, vol. 19, no. 5, pp. 835-867, 2011.
6. Hsien-Ming, H., Yeali, S., Meng, C.-C., "Collaborative scheme for VoIP traceback", *Digital Investigation*, vol. 7, nos. 3-4, pp. 185-195, April 2011.
7. I-Long, Lin, Yun-Sheng, Y. "VoIP Digital Evidence Forensics Standard Operating Procedure", *International Journal of Research and Reviews in Computer Science*, vol. 2, no. 1, pp. 22-38, 2011.
8. Irwin, D., Slay, J., "Extracting Evidence Related to VoIP Calls", *Advances in Digital Forensics VII*, IFIP AICT 361, pp. 221-228, 2011.
9. Stachtari, E., Soupionis, Y., Katsaros, P., Mentis, A., Gritzalis D., "Probabilistic model checking of CAPTCHA admission control for DoS resistant anti-SPIT protection", in *Proc. of the 7th International Workshop on Critical Information Infrastructures Security*, pp. 143-154, Springer (LNCS 7722), Norway, 2012.
10. Soupionis, Y., Gritzalis, D., "Audio CAPTCHA: Existing solutions assessment and a new implementation for VoIP telephony", *Computers & Security*, vol. 29, no. 5, pp. 603-618, 2010.
11. Soupionis, Y. Tountas, G., Gritzalis, D., "Audio CAPTCHA for SIP-based VoIP", in *Proc. of the 24th International Information Security Conference*, pp. 25-38, Springer (IFIP AICT 297), 2009.