A Regulator's Perspective to Communication Security.

Ioannis Psallidas, Vassilis Stathopoulos, Sotiris Maniatis
Hellenic Authority for Communication Security and Privacy
Ierou Lohou 3, Marousi 151 24, Athens, Greece
Psallidasi@adae.gr, StathopoulosV@adae.gr, ManiatisS@adae.gr

***Abstract*— The Hellenic Authority for Communication Security and Privacy (ADAE) is mandated to secure electronic communications in Greece both in terms of protecting the confidentiality and availability of relevant networks and services. It issues rules and regulations that all parties concerned need to comply with. Through compliance audits and complaint investigations, weaknesses are identified in electronic Communication Service Provider (CSP) offerings that need to be rectified. Major issues of concern such as unlawful interception of mobile phone communications, evidence of serious vulnerabilities of extensively operated protocols, such as SS7, improving network and service availability through CSPs' system outages and service disruptions auditing and information exchange, cross country authority collaboration in dealing with communication services security auditing and end user complaint investigation are elaborated. Cloud computing is supposed to be used extensively in the next few years, but there are still concerns on communications privacy related issues and from a regulatory point view.**

Keywords*— *Communications Privacy; Security; Availability; Regulation; Audits; Investigation;Challenges.

I. INTRODUCTION

Unlawfully intercepted communications is one of the hottest topics in the news, especially after Edward Snowden's revelations of alleged USA National Security Agency (NSA) electronic communications eavesdropping back in 2013 [1]

Communication confidentiality is a very sensitive topic in Greece, to a point that the Greek constitution makes specific references to its safeguarding. As a result, the Hellenic Authority for Communication Security and Privacy (ADAE) was established in 2003.

Since 2013 ADAE has also taken up the responsibility of issuing regulation that CSPs need to adopt in order to ensure the continuity and availability of their network and services to acceptable levels.

In order to fulfil its purpose, it audits all parties concerned in a proactive fashion and investigates reported incidents and end user complaints.

Unlawful interception of mobile phone communications has also been a concern to other authorities all over Europe. A systemic network wide approach involving all the necessary mobile network intelligence components is one of the options that could be investigated, but the participation of vendors, network providers and regulators is essential.

Regardless of what security assurances mobile network operators provide, there is hard evidence that in fact proves how vulnerable supporting systems are. In 2014, the media reported an SS7 protocol vulnerability by which non-state actors can track the movements of cell phone users from virtually anywhere in the world.

The major business commitment of each CSP is to offer highly available communication services. This requires the network administrators' quick response to security incidents that affect their network systems and their available services. CSPs may underestimate some incidents or lack of combined analysis that requires the consolidation of the incidents. It is also desirable by regulatory bodies to have better feedback of network availability performance, both in terms of information quality and level of detail.

The new paradigm regarding the provision of communication services is to expand to more than one nation, acquiring economies of scale. For example, big telecommunication companies that operate in Europe utilise big data centres that host information and communication systems which serve big regions that extend to many countries. In addition, over-the-top communication services, like Skype, are global in nature. Auditing of such services is complicated due to different legal and regulatory frameworks, necessitating the cooperation of all involved regulators.

Even though Cloud computing utilises processing economies of scale, flexible resource allocation, and heightened availability, there is concern of true tenant information isolation and isolated tenant auditing, especially if higher levels of the Cloud paradigm e.g. PaaS and SaaS are adopted by end users.

The paper first addresses background information on ADAE's mandates, activities, regulations and experience. Then, it provides a discussion on the major issues of concern mentioned above.

II. THE HELLENIC AUTHORITY FOR COMMUNICATION SECURITY AND PRIVACY.

The Hellenic Authority for Communication Security and Privacy (ADAE) [2] has been established according to article 19 par. 2 of the Greek Constitution. Article 1 of its founding law, 3115/2003, states that its purpose is to protect the correspondence or communication in any possible way. By electronic communications privacy one refers to keeping both the content of an established communication and the relevant

generated communication data (such as the time the communications started, its time duration, the calling and receiving party numbers and / or location etc) confidential.

Additionally, law 4070/2012 awarded ADAE the mandate of gauging the electronic CSP market regarding its capability of delivering communications services continuously to the subscriber base, by issuing relevant regulation and performing compliance verification. It complements the Greek National Regulatory Authority's (NRA) [3] overall responsibility of overseeing the Greek Telecommunication market in matters of quality of service. Any compliance audit or incident response reports generated by ADAE are forwarded to the Greek NRA for further administrative disciplinary action.

ADAE is an independent authority under parliamentary scrutiny. An annual report is submitted to the Parliament President, Minister of Justice, Transparency and Human Rights, leaders of elected political parties and the European Parliament.

In order to fulfil its purpose, it audits all parties concerned in a proactive fashion and investigates reported incidents and end user complaints. The outcome of these audits and investigations is twofold. To discipline through administrative fines and recommendations, making the market more security-wise cultured and mature, and for the authority itself, to adapt its security regulatory posture against electronic communication technology's accelerated evolution.

III. ADAE'S REGULATORY FRAMEWORK.

A. *Communication Confidentiality.*

Over the last 13 years ADAE has established rules and regulations that both electronic Communications Service Providers and Law Enforcement Agencies (LEAs) need to comply with in order to safeguard electronic communications privacy and at the same time oversee Lawful Interception when circumstances require for such action. So far, two major sets of regulations regarding the safeguarding of electronic communications privacy have been issued by the Authority. The first set was issued late in 2005 and was technology specific. There was a different subset of regulations for safeguarding the confidentiality of legacy type of electronic communication services (fixed telephony, mobile telephony, fixed point to point communication services, wireless communications, satellite communications etc) from IP protocol or Internet based communication services. After a seven year enforcement of these regulations through relevant compliance audits, incident investigations and hearings performed by the Authority, and taking into consideration both, the fast technology paradigm shift, whereby the Internet Protocol was becoming the preferred communications platform, and relevant EU legislative amendments [5] [6] [7], it was decided to revise the regulations, and following a public consultation a new, technology agnostic, unified set was introduced in late 2011 known as ADAE decision 165/2011 [8].

B. *Security and Availability of Networks and Services of Electronic Communications*

Based on the mandate given to ADAE by law 4070/2012, and following a public consultation, a regulation known as ADAE decision 205/2013 [9] was issued, which electronic CSPs need to adopt in order to strengthen the continuity and availability of their network and services to acceptable levels.

IV. AUDIT AND INVESTIGATION FINDINGS

ADAEs primary tools are audits and investigations. Audits are used for regulatory compliance checks and for discovering security policy implementation effectiveness or regulatory compliance deficiencies. Investigations are used for seeking the necessary forensic evidence for proving communication security wrong doings from the CSPs' part.

A. *Communication Confidentiality*

So far all major CPSs have gone though at least one exhaustive regulation 165/2011 based compliance audit and numerous incident or complaint investigations. Most frequent security issues discovered are un-patched software, non-adherence to security procedures, utilising systems for which security was not considered in the development and / or implementation phase, non adoption of command and event logging especially true for small size security-immature providers.

The crown jewel of these efforts is a case [10] where it was discovered that the mobile phones of a number of members of the Greek government and top-ranking civil servants, where shadowed and the content of their conversation was unlawfully intercepted. The investigation performed by ADAE lead to evidence that confirmed the unlawful act and the CSP involved was eventually awarded an administrative fine of 50.6 million euros.

B. *Security and Availability of Networks and Services of Electronic Communications*

At this stage of its adoption, mainly the top 8 major CSPs have been audited, with the intent of "nudging" the market in taking the necessary preliminary steps for implementing what is required in order to achieve full regulatory compliance. By this, all major CSPs must have at least gone through the phase of performing Business Impact Analysis and Risk Assessment whereby risk relevant to continuity is identified, analysed and evaluated. The first round of audits has proven this to a satisfactory degree. The next step is for the electronic communications market to prove that it has adopted all necessary controls and put in place all necessary processes in order to monitor, review and adapt its network and services availability posture.

V. ISSUES OF CONCERN.

Some of the major issues of concern are unlawful interception of mobile phone communications, evidence of serious vulnerabilities of extensively operated protocols, such as SS7, improving network and service availability through CSPs' system outages and service disruptions auditing and

information exchange, cross country authority collaboration in dealing with communication services security auditing and end user complaint investigation. Although Cloud computing is supposed to be extensively adopted in the next few years, there are still many concerns on communications privacy related issues.

A. *Interception of mobile communications*

Interception of mobile phone communications has always been a concern. During the last years, a few incidents have been reported in the media, concerning potential interception of mobile communications through false base stations (otherwise called IMSI catchers). The use of such devices is legal when used by national agencies under specific provisions and procedures of law, but it is illegal when used by individuals.

Indicatively, Norway's newspaper Aftenposten, in December 2014, has written articles about the discovery of false base stations in downtown Oslo. Apparently, in March 2015, investigations from the Norwegian Police Security Service (PST) showed that, although no indications have been found on the use of false base stations based on the material provided by Aftenposten, such base stations have been used in other cases in the past, and therefore the overall issue cannot be demoted.

The threat of mobile communications interception is apparent especially in second generation (2G) networks that make use of protocols and algorithms, that could be considered ambitious for their time (late 1980s), but they are now surpassed by the enormous progress in computational power. Of course, the same threats are relevant also to newer generations of mobile networks.

One possible solution to the aforementioned threat is to adopt a systemic network-wide approach involving all the necessary mobile network intelligence components. Specially designed software and hardware probes could be installed in the components of the operators' mobile networks, for example to measure variations in the air interface or to observe strange protocol behavior, which could provide real-time (or near real-time) indications that such devices are operating and set an alarm. In order to set up such capacities, the participation of vendors, network operators and regulators is essential, which complicates the effort and increases the costs.

Another solution would be to follow a hardening approach of the mobile network by choosing the necessary configuration options already supported by the protocols [11]. Initially, interventions must be performed in the cryptographic and ciphering algorithms used for user authentication and over-the-air encryption. For example, the GSM Milenage algorithm [12] could be enforced as the A3/A8 function in GSM. Another example is to totally forbid the use of the A5/2 algorithm and specify A5/3 as the preferred algorithm for over-the-air encryption. Other interventions involve signalling options, like for example the frequency of identifiers' reallocation, the control of the Short Message Service and the SIM/USIM configuration.

B. *SS7 Security Issues*

Signalling System No.7 (SS7) is a set of layered protocols that is used to transfer signalling information among elements of the network to provide services to subscribers, for example to setup calls or to handle roaming. The SS7 set of protocols was designed at a time when security was not the primary concern, since providers were based on mutual trust to exchange information. The adoption and use of SS7 by mobile networks, the need for global communications as well as the proliferation of new mobile services (e.g. location-based services) has opened up access to SS7 interfaces to a vast number of actors. The trust-based model is not adequate anymore to cater for the emerging security threats.

Actually, there is hard evidence that in fact proves how vulnerable SS7 supporting systems are. In 2014, the Washington Post published two articles about location tracking and interceptions [13], [14]. Moreover, in 2014, there were papers and presentations about the vulnerabilities of the SS7 protocol [15], [16].

In brief, the main threats that were reported are related to user location tracking, intercepting calls, SMSs or internet traffic, performing Denial of Service (DoS) attacks to subscribers and the network, making illegitimate calls thus avoiding charges and sending unsolicited messages.

In order to mitigate these threats, the most effective way would be to totally rely on a next generation protocol that would be designed with inherent security (authentication, encryption). The drawback is that this would require a lot of time and cost to be deployed.

Until then, there are a number of measures that providers could take to harden their signalling systems, in terms of optimal configuration, logging and examining of suspicious SS7 traffic and firewalling based on message type and source address. For example, operators could block at their network border Mobile Application Part (MAP) messages that originate from outside networks but are intended to be used only internally. Further, operators could configure SMS home routing and avoid the use of Optimal Call Routing, among others.

ADAE is in the process of investigating appropriate regulatory provisions in order to mitigate the threats that relate to both interception of mobile communications and SS7 security issues, in cooperation with the providers of mobile communications that operate in Greece..

C. *Security and Availability of Networks and Services of Electronic Communications*

Reliable and secure internet and electronic communications are now central to the whole economy and society in general. These goals require Providers of electronic communications to attach particular importance to their network and services' availability. Developed procedures should be kept updated, exercises should be executed and important plans such as business continuity plans that challenge the Providers' security reflexes against serious security incidents should be frequently tested and evaluated. Hence, in case of incidents' occurrence, the Provider with

decisive steps and qualitative restoration actions should maintain high network and service availability.

Large and serious outages usually receive close attention by Providers while their technical teams share the produced knowledge by facilitating the industry to understand and encounter these security incidents. EU pays further attention to such incidents by fostering the legal framework. Indeed, EU decided to add article 13a to the Framework directive [7], regarding security and integrity of public electronic communications network and services. Among others, article 13a states that Providers must report significant security breaches to national competent authorities.

However, many smaller outages remain undetected and if detected, patchwork solutions may be applied without offering long-term solutions. Similar incidents in terms of cause, root cause or the nature of the incident may be repeated many times. Technical teams are not always able to show the necessary significance in collecting and processing this information by resulting in faulty decisions that may affect the network and service availability. In general, lack of information and lack of transparency about communication network and service incidents makes it difficult for policy makers to understand the overall impact, the root causes and possible interdependencies.

Overcoming this weakness, means that each time a new incident is encountered, information should be collected by recording the maximum possible technical details that determine the anatomy of the incident. Details should be focusing on

- accurately specifying the network area (i.e. access, aggregation, edge, core layers) that the incident occur,
- the respective system (switch, router, BRAS, etc) that causes the incident and the system that is affected,
- the geographical features of the affected area (i.e. island area or mainland),
- the technical cause and technical effect of the incident,
- mean number of the affected subscribers.

One obstacle that must be overcome is that all Communication Providers should adapt to the same methodology, for example the segmentation of their network to network areas should use the same principles, or the affected subscribers should be estimated under the same methodology.

D. Cross Border Cooperation

Article 13a of the EU Framework Directive (Framework Directive 2002/21/EC as amended by Directive 2009/140/EC) [7], requires electronic communications providers to assess risks, take appropriate security measures to prevent security incidents, and report on security incidents to their national regulator. This triangle of activity is generally supervised by a telecom regulator, which has the challenging task of supervising security across a sector of service providers consisting of hundreds of businesses ranging from very small operators to large multinationals who have infrastructure across borders. In case of small operators that keep their infrastructure within their premises or at least have granted pieces from their services' implementation to third parties but always operating within the national borders, supervision is completed by following the scheduled audit procedures. Security supervision of large multinational providers that distribute part of their infrastructure across national borders is a challenge for the auditors, especially when on-site audits for receiving evidences are required and real time answers received by the personnel and the security officer ought to be collected.

Similarly, the e-Privacy Directive [5][6] asks providers to take appropriate security measures to protect their personal data and report on data breaches to their national regulator. The e-Privacy Directive applies only to traditional telecom providers, and not to over-the-top service providers that provide communications services such as Voice over IP, instant messaging and emailing over social networks.

Auditing of multinational providers (i.e. over-the-top service providers, cloud computing providers), means either executing proactive audits for ascertaining the Provider's security level or executing reactive audits for investigating a security incident. Both proactive and reactive audits should be executed across national borders. But auditors from one member state do not have the authority to travel across borders and audit the premises of multinational providers in another member state. Moreover, big multinational providers keep a complex and continuously changing network. Hence it becomes difficult for an external auditor to assess the security of such a changing environment. Finally a heterogeneous legal and regulatory framework among the EU member states also puts a further constrain.

Above mentioned Directives do not have any provisions for solving such problems. The General Data Protection Regulation 679/2016 [17] that authorizes only Data Protection Authorities for the processing of personal data, includes three important articles, that is, articles 60, 61 and 62 that are about cooperation, mutual assistance and joint operations of these supervisory authorities. In view of the fact that in some jurisdictions of the EU the authorities which are competent for the provisions of the e-privacy Directive and the Article 13a of the Telecom Package (Authorization and Access Directive) are other than the Data Protection Authorities, it is of fundamental importance to provide for an effective mechanism of direct cooperation and mutual assistance (information requests, supervisory measures, inspections etc) with the direct participation of these competent authorities.

Following a list of the required improvements that both the e-privacy Directive and the Authorization and Access Directive could include:

- Multinational providers, cloud computing providers and government authorities should establish a continuous program of monitoring, audits, even tests and exercises in place [18].
- a common homogenized framework that will adopt a set of minimum security measures legitimized for all member states

- build Joint operations procedure of the competent authorities of different member states that will fulfil the need of implementing common audits, investigations and for monitoring the implementation of security measures of Communication Providers,
- mutual assistance and cooperation between the competent authorities that will cover information requests to carry out prior consultations, inspections and investigations.

E. Cloud Computing

Even though Cloud computing utilises processing economies of scale, flexible resource allocation, and heightened availability, there is concern of true tenant information isolation and isolated tenant auditing, especially if higher levels of the Cloud paradigm e.g. Platform as a Service (PaaS) and Service as a Service (SaaS), are adopted by end users. This is true when trying to draw up regulation regarding e.g. communication data retention. The market wants to take advantage of the operational and economical benefits of such technologies and possibly come up with solutions that cater for communication data retention needs of multiple CSPs, in a shared resource but logically separated multitenant environment solution offerings. On the other hand this technology might not guarantee the separation of such confidential data amongst resource sharing CSPs yet. The other issue of concern is, when auditing a CSP that is using systems which are shared amongst multiple tenant CSPs, whether the collected evidence from these shared resources, contains information regarding CSPs that are not being audited.

VI. CONCLUSIONS

The Hellenic Authority for Communication Security and Privacy is continuously working to ensure that the Greek CSP market achieves high levels of maturity in terms of confidentiality and availability of electronic communications, by keeping up-to-date with the technological and regulatory current affairs.

It investigates possible solutions for unlawful mobile phone communication interception countermeasures and SS7 vulnerability cures, being open to any form of cooperation to these ends. It has scheduled an open consultation regarding the gathering and retention of useful data related to network and services availability in order to be able to reach informed conclusions and possible regulatory actions. It continuously seeks ways to improve cross boarder cooperation amongst relevant regulatory authorities, to protect the fundamental right of communication confidentiality and ensure high levels of end-to-end service availability through information sharing. It follows closely the introduction of new technologies that will have a significant impact to future service offerings.

References

[1] "Edward Snowden: Leaks that exposed US spy programme," 17 January 2014. [Online]. Available: http://www.bbc.com/news/world-us-canada-23123964.

[2] "Hellenic Authority for Communication Security and Privacy," [Online]. Available: http://www.adae.gr/en/

[3] "Hellenic Telecommunications & Post Commission," [Online]. Available: http://www.eett.gr/opencms/opencms/EETT_EN/index.html.

[4] "Greek Parliament's Conference of the Presidents body," [Online]. Available: http://www.hellenicparliament.gr/en/Organosi-kai-Leitourgia/Diaskepsi-Proedron/.

[5] DIRECTIVE 2002/58/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications).

[6] DIRECTIVE 2009/136/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 25 November 2009 amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services, Directive 2002/58/EC concerning the, processing of personal data and the protection of privacy in the electronic communications sector and Regulation (EC) No 2006/2004 on cooperation between national authorities responsible for the enforcement of consumer protection laws.

[7] DIRECTIVE 2009/140/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 25 November 2009 amending Directives 2002/21/EC on a common regulatory framework for electronic communications networks and services, 2002/19/EC on access to, and interconnection of, electronic communications networks and associated facilities, and 2002/20/EC on the authorisation of electronic communications networks and services.

[8] "Regulation for the Assurance of Confidentiality in Electronic Communications," [Online]. Available: http://www.adae.gr/fileadmin/docs/nomoi/kanonismoi/ADAE_REGULATION_165.2011.pdf.

[9] "ADAE Decision 205/2013, Regulation for the Security and Integrity of Network and Services of electronic communications," [Online]. Available: http://www.adae.gr/fileadmin/docs/nomoi/kanonismoi/Kanonismos_FEK_1742_B_15_07_2013_asfaleia_akeraiotita__ADAE_205_2013.pdf.

[10] "Court upholds 50.6 mln penalty for Vodafone in wiretapping scandal" 7 December 2015. [Online].Available: http://www.ekathimerini.com/204115/article/ekathimerini/news/court-upholds-506-mln-penalty-for-vodafone-in-wiretapping-scandal

[11] G. M. Koien, "A Best Current Practice for 3GPP-based cellular system security," in 4th International Conference on Wireless Communications, Vehicular Technology, Information Theory and Aerospace & Electronic Systems (VITAE), May 2014.

[12] 3GPP TS 55.205, "Specification of the GSM-MILENAGE algorithms: An example algorithm set for the GSM Authentication and Key Generation Functions A3 and A8".

[13] C. Timberg, "For sale: Systems that can secretly track where cellphone users go around the globe," 24 August 2014. [Online]. Available: https://www.washingtonpost.com/business/technology/for-sale-systems-that-can-secretly-track-where-cellphone-users-go-around-the-globe/2014/08/24/f0700e8a-f003-11e3-bf76-447a5df6411f_story.html.

[14] C. Timberg, "German researchers discover a flaw that could let anyone listen to your cell calls," 18 December 2014. [Online]. Available:https://www.washingtonpost.com/news/the-switch/wp/2014/12/18/german-researchers-discover-a-flaw-that-could-let-anyone-listen-to-your-cell-calls-and-read-your-texts/.

[15] E. Tobias, ""SS7: Locate. Track. Manipulate."," in 31C3, Hamburg, December 2014.

[16] N. Karsten, ""Mobile self-defense"," in 31C3, Hamburg, December 2014.

[17] REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Da, (General Data Protection Regulation) .

[18] Enisa, Critical Cloud Computing, A CIIP perspective on cloud computing services , version 1,0, December 2012.

Biographies of authors

Ioannis Psallidas (CISSP, CISA, CRISC, COBIT5F) received both the Bachelor of electrical and computer systems engineering and Master of Engineering Science degrees from Monash University -Melbourne Australia, in 1996. Started as a telecoms engineer focusing on the technical side of telecommunication provider operations, then moved on with facilitating the liaison of higher level business objectives and the underlying technical aspects through a number of mid to senior management positions at various telecommunications companies. Since 2008 holds the position of the Director of the Assurance of Infrastructures and Privacy of Services and Internet Applications Division at the Hellenic Authority for Communication Security and Privacy.

Vassilios Stathopoulos received his B.Sc. degree in Physics from University of Athens at 1996, his M.Sc. degree in Communication, Control and Digital Signal Processing from University of Strathclyde, Glasgow, UK at 1997 and his PhD degree from National Technical University of Athens (NTUA) at 2001. He has also been participating, as research associate, in several European Projects until 2005. Since 2005, he has been working for ADAE "Hellenic Authority for Communication Security and Privacy" as a security expert and he also holds the position of head of the Department of security audit of systems and services.

Sotiris Maniatis received a Diploma degree in computer engineering and informatics from the University of Patras, Greece, an M.Sc. degree in information systems engineering from UMIST, United Kingdom, and a Ph.D. degree from the School of Electrical and Computer Engineering of the National Technical University of Athens (NTUA) in 2002. He has been a research associate in the telecommunications laboratory of NTUA and participated in several academic research projects until 2005. Since then, he works for the Hellenic Authority for Communication Security and Privacy and he is currently the head of the Department of Internet Infrastructures.