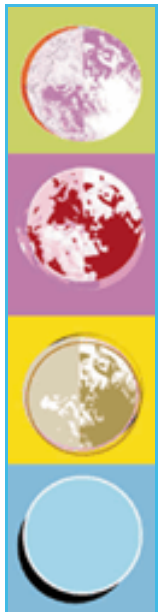


Regulatory Framework for Communications Security and Privacy in Greece

Georgia Bafoutsou, Nikolaos Antoniadis, Eugenia Nikolouzou, Athanasios Panagopoulos

Authority for the Assurance of Communications Security and Privacy (ADAE)

http://www.adae.gr

3 Ierou Lochou str., 15124 Maroussi, Greece

{bafoutsoug, antoniadisn, nikolouzoue, panagopoulosa}@adae.gr

Presentation Overview

- This presentation provides an overview of the Regulatory framework set up by ADAE, in the context of electronic communication providers. Special attention will be given to the following:
  - The outcome: two years after the application of the regulatory framework
  - Subscribers complaints
  - Acts published
  - Lawful Interception and Data Retention
  - Future Issues

The scope of ADAE

- ADAE is the Greek Independent Regulatory Authority for the Information and Communication Security and Privacy
  - ADAE has been established by Article 1 of the law 3115/2003, following the guidelines set in paragraph 2 of the article 19 of the Greek Constitution,
- The objective of ADAE is to protect the Secrecy of Mailing, the Free Correspondence or Communication in any possible way as well as the Security of Networks and Information.
- In this context, ADAE has issued Regulations concerning the Assurance of Communications' Privacy in fixed, mobile, wireless and Internet communications.
  - These Regulations enforce the application of technical, organizational and procedural security measures in electronic communication providers.
  - They define a security life-cycle, including the definition of a Security and Privacy Policy by each provider, the application of the required security measures and the auditing procedure through which the Authority which will verify the appropriate implementation of the defined policies.

Regulatory Framework (1/3)

- ADAE Regulations are mainly based on the standards
  - BS 7799-2:2002
  - ISO/IEC 17799:2000
  - ITU-T X.1051

- The Electronic Communication Providers shall develop, implement, maintain and continually improve a documented security policy that should contain at least:
  - Access Policy: that defines the access and authorization level that each user requires for accessing the provider's assets.
  - Acceptable Use Policy: that defines the allowed or the not allowed activities of each user.
  - Protection of Telecommunication Network Policy (Core, Access): includes protection of network abnormal situations, vulnerabilities of interconnected networks, external attacks and physical security.
  - Communications Data Processing Security Policy : concerns security measures necessary to ensure protection of communication data.
  - Protection of the Internal Telecommunication Network: concerns handling of communication data on behalf of providers' associates and personnel.

Regulatory Framework (2/3)

- **Application Service Provider Security Policy**: defines the set of warrants that the service provider requires to get from the application service provider in order to assure the users' communication privacy.
- **Back-up Security Policy** : describes all the required procedures that assure the recovery of communication infrastructure within a logical period of time after the occurrence of any damage.
- **Protection and Virus Deterrence Policy**: defines the deterrence, tracing and confront procedures from viruses.
- **Password Use Policy**: defines the creation, management and protection procedures regarding passwords usage.
- **Perimeter Security Policy**: defines the appropriate mechanisms for protecting internet providers' assets from outside or inside attacks (firewalls, IDSs, e.t.c).
- **Security Incident Handling Policy** : defines a procedure for recording the incidents, notifying the relative organisations and examines all elements for identifying possible mistakes.

Regulatory Framework (3/3)

- **User Ethics Policy**: defines a set of morality rules regarding the provider and the user, for assuring the communication privacy.
- **Third Party Agreements Policy** : defines the agreement framework, between a service provider and a subcontractor, for a project undertaking that requires access towards the service provider critical assets that is obliged to assure.
- **Management and Installation of Telecommunication Infrastructure Policy** : that assures the communication privacy when changes or insertion of new communication infrastructure takes place.
- **Network Security Audit Policy**: mainly defines a team that uses special security audit software for scanning internet providers' assets for assuring their integrity confidentiality and availability.
- **Risk Assessment Policy** : defines the procedure of identification, audit and evaluation of the vulnerable assets and vulnerable access points regarding the hardware and software infrastructure for minimizing the violation probability.
- **Internet User Security Policy**: defines the rules and the security requirements for the usage of internet as a secure medium for the communication of sensitive information.
- **Lawful Interception Security Policy**: concerns the obligations on behalf of the providers regarding the management of LI systems.

Telecommunication Regulatory Framework

- Assurance of Privacy Protection during the Provision of Telecommunication Services through Networks of Mobile Communications, Wired Networks and Wireless Networks
- The clauses of these regulations concern all telecommunication services providers
- Vulnerable points:
  - Terminal equipment (cellular device, file of incoming and outgoing calls, SIM, telephone device, machine, etc)
  - Network Elements and Services (Base Stations, Mobile Switching Centers, Telephone Network Interface Box - TNI-Box, Access Points, servers, hub station, satellite terminals)
  - Outdoor switches-KV,
  - Switching centers, central switches and gateways
  - Cryptographic Algorithms, Interconnection Points with Fixed Networks etc.).
- Common Threats:
  - the obtainment of access in the core network,
  - denial of service of an interfered subscriber,
  - attack on the SIM/USIM card,
  - man-in-the middle attacks,
  - attacks on the access points, satellite terminals, and cryptographic algorithms.

Internet Regulatory Framework

- Assurance of Privacy Protection during Internet Communications
- The scope of this regulation concerns every Internet Service Provider, Application Service Provider and Added Value Service Provider referred to them as Internet Providers.
- Vulnerable Assets:
  - Terminal Equipments
  - Network Elements (Routers, Switches or Gateways)
  - IT nodes and servers (Email servers, web servers etc)
  - Their respective system or application Services.
- Common threats:
  - Viruses
  - Worms
  - Application or System Vulnerabilities Exploitation.

Application of Regulations

- 350 registered Internet and Telecom Providers (based on the Annual Report 2005 of EETT) that apply on ADAE regulations
- 26% of them submitted security policies to ADAE for review
  - Accepted security policies concern almost 90% of the Internet and Telecom Market
  - 30% of the submitted policies complied with the regulations
- 74% Internet and Telecom Companies have not submitted security policy
  - Rapid changes in the electronic communications market
  - Resellers of electronic services
  - Headquarters located outside of Greece
  - Difficulty in combining the scope of regulations with EETT registry
- Next step is the implementation of the regulations
  - ADAE will audit the security policies application

Subscribers' complaints

- From the total number of subscribers' complaints concerning Internet, Telecom and Mailing Services
  - 13% do not fit in ADAE responsibility
  - 90% concern Telecommunications
- The majority of complaints is about service or network malfunctions misunderstood from users

E-112 Emergency Calls Handling

- A new Regulation has been recently published by ADAE regarding the processing of caller location information in electronic communication networks for the purpose of location-enhanced emergency call services (112 Call).
- Applied only to Fixed and Mobile Telephony Providers
- "Pull solution" (cell id, base station coordinates, azimuthal angle of main antenna lobe) in use from 19/12/2006.
  - General Secretariat of Civil Protection receives an emergency call
  - They request caller location information from telecom providers (telephone, email, fax)
  - Telecom providers are obliged to supply the information as soon as possible
- Network Identifier Transmission is necessary to take into account for the special cases of calling 112 without SIM and Radio Coverage
- Obligations for Calling Line Identification (CLI) have been stated.

E112 Emergency Calls Handling

- Access Policy, Acceptable Use Policy, Processed Data Management (deletion, storage, etc)
- Regular audits to the Civil Protection and Telecom Providers
- Annual Statistics of the Telecom Providers Response Time to the "Pull" Solution
- "Push Solution" (accurate coordinates, automatic transfer of to the Civil Protection's Call Center)
  - Location Based Services are not provided by the Greek Telecom Providers
  - 3G Radio coverage has not yet been developed in rural areas

Malicious Calls

- ADAE has published act regarding the elimination of the presentation of calling line identification,on a temporary basis, upon application of a subscriber requesting the tracing of malicious or nuisance calls.
  - The subscriber submits a relative application to the provider.
  - The provider is obliged to give the list of incoming calls for a future period of maximum 15 days.
  - No caller identity information is provided.
  - During the period of the CLI elimination all callers are notified appropriately with the use of a recorded message.

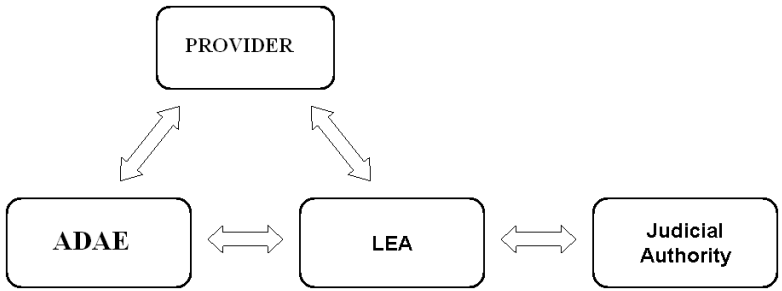
- Providers are subject to ADAE audits

Waiving of Privacy Protection Rights

- A Law Enforcement Agency (LEA) requests a warrant for the retrieval of retained data of a particular subscriber from the Judicial Authority. LEA requests the information retained about a specific target from the provider by supplying the appropriate warrant, manually signed by the Judicial Authority.

- Once the provider accepts and validates the request, the information is delivered to the LEA, which can use it for its investigative purposes and for submission as evidence in court.

- LEAs and the Providers are directly audited by ADAE for the above procedure.



Data Retention

- At present, ADAE, Ministry of Justice, LEAs and the involved providers are discussing open issues concerning the Data Retention directive implementation
  - data retention for unsuccessful calls
  - double records
  - security architectures
  - costs
- ADAE will possibly contribute in technical terms on publishing a new regulation regarding Data Retention Directive
  - access issues
  - retention time
  - storage of data
  - deletion of data
- LEAs and the Providers will be directly audited by ADAE for the above procedure.

Lawful Interception Current Status

- ADAE has the role of coordinator between LEAs and Providers
  - After several meetings both sides agreed to apply ETSI standards in LI field.
- Most Telecom and Internet providers have already installed the necessary modules.
- Operation tests have not been performed yet.
- Open Issues
  - Lawful Interception Identifier (LIID) has not been identified yet.
  - The Type of Interconnection (leased lines, through public switched telecommunication network, etc) between the Providers and the LEAs and the security measures for HI2 and HI3 interfaces have not been fully agreed yet.
  - Security requirements at the interface ports HI2 and HI3 should be discussed and issues like Authentication, Confidentiality and Integrity addressed

Future Issues

- Data Retention Directive implementation
- Providers security policies for log file management
- Information Society Project
  - Creation of ADAE portal for interaction with citizens and providers
  - Workshops to inform citizens about security and privacy in electronic communications
- Emergency Calls push solution
- Li testing and operations between LEAS and Providers
- On site audits of Electronic Communication Providers Security Policy Implementation
- Regulation review and adaptation to the current technological status.