# A Regulator's Perspective to Communication Security

Ioannis Psallidas, Vassilis Stathopoulos, Sotiris Maniatis

**Ioannis Psallidas** CISSP,CISA,CRISC,COBIT5F
Director
Assurance of Infrastructures, Privacy of Services & Internet Applications
**Hellenic Authority for Communication Security & Privacy**

# Agenda

i. The Hellenic Authority For Communication Security And Privacy (ADAE).

ii. ADAE Regulatory Framework.

iii. Audit And Investigation Findings.

iv. Issues of Concern.

# ADAE Mission

To Secure Communication Privacy.

To ensure the Security and Integrity of Networks & Elec. Comm. Services.

# ADAE Operational Framework

ADAE is an Independent Authority.

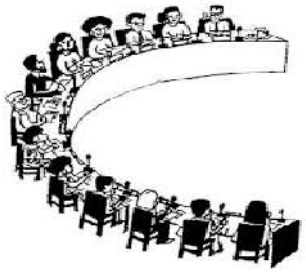

Undergoes Parliamentary Scrutiny as per Parliament Rules and Regulations.

Performs Scheduled and Unscheduled Audits either after Planning, Incident reporting or Complaint lodging.

Partakes in Law drafting and Issues Rules and Regulations

ΕΦΗΜΕΡΙΔΑ ΤΗΣ ΚΥΒΕΡΝΗΣΕΩΣ ΤΗΣ ΕΛΛΗΝΙΚΗΣ ΔΗΜΟΚΡΑΤΙΑΣ

# ADAE Operational Framework



Performs Hearings.

Cooperates with other Authorities & Organizations both Domestically and Internationally.

# Agenda

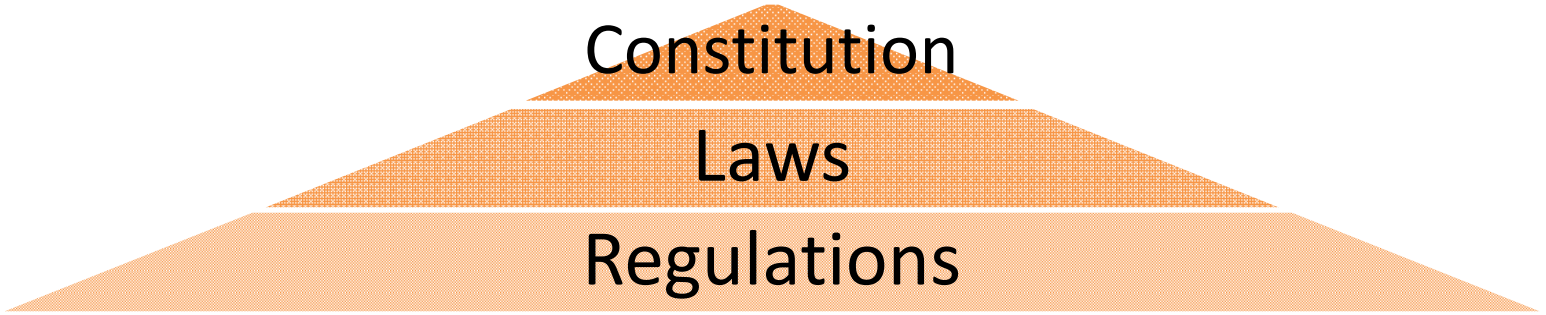
i. The Hellenic Authority For Communication Security And Privacy (ADAE).

ii. ADAE Regulatory Framework.

iii. Audit And Investigation Findings.

iv. Issues of Concern.

# ADAE Regulatory Framework




**ADAE Decision 165/2011**

Regulation for the Securing Electronic Communications & Privacy

**ADAE Decision 205/2013**

Regulation for the Security and Integrity of Networks & Elec. Comm. Services

These Regulations enforce the implementation of

- Organizational structures,
- Procedures and
- Technical measures

It is Mandatory for Service Providers to have Security Policies / Measures that reflect on the above regulations.

# Agenda

i. The Hellenic Authority For Communication Security And Privacy (ADAE).

ii. ADAE Regulatory Framework.

iii. Audit And Investigation Findings.

iv. Issues of Concern.

# Audit and Investigation Findings.

**ADAE Decision 165/2011**

Regulation for the Securing Electronic Communications Privacy

Most frequent security issues :

- 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 access, command and event logging
  - especially true for small size security-immature providers

# Audit and Investigation Findings.

**ADAE Decision 165/2011**

Regulation for the Securing Electronic Communications Privacy

Crown jewel of cases :

In 2004, 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

# Audit and Investigation Findings.

**ADAE Decision 205/2013**

Regulation for the Security and Integrity of Networks & Elec. Comm. Services

Top 8 major CSPs have been audited :

- "Nudge" the electronic communications market.
- Must have performed Business Impact Analysis and Risk Assessment.
- The first round of audits has proven this to a satisfactory degree.
- The next step is for the 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

# Agenda

i. The Hellenic Authority For Communication Security And Privacy (ADAE).

ii. ADAE Regulatory Framework.

iii. Audit And Investigation Findings.

iv. Issues of Concern.

# Issues of Concern

- Interception of Mobile Communications.
- SS7 Security Issues.
- Availability of Networks and Services Intelligence
- Cross Border Cooperation.
- Cloud Computing

# Issues of Concern

## Interception of Mobile Communications

- IMSI catchers are legal when used by national agencies under specific provisions and procedures of law, but are illegal when used by individuals.
- Problem with earlier generation networks.
- Interception difficulty increases with the adoption of newer Generation networks.

# Issues of Concern

## Interception of Mobile Communications > Solutions

| System Network-wide | Mobile Network Hardening |
|---|---|
| Detective | Preventative |
| HW & SW probes monitoring e.g.<br>• variations in the air interface<br>• strange protocol behaviour,<br>could provide real-time (or near real-time) indications of foreign network elements. | Choose the necessary configuration options already supported by the protocols.<br>• CSP dependent Crypto/Cipher A3/A8 function -> GSM Milenage.<br>• Over-the-air encryption A5/2 -> A5/3 |
| High complexity, Capital Intensive | |
| Participants : Vendors, Network operators, Regulators | |

# Issues of Concern

## SS7 Security Issues.

- SS7 was designed when security was not the primary concern.
- SS7 interfaces are open to a vast number of actors.
  - need for global communications
  - proliferation of new mobile services (e.g. location-based services)

# Issues of Concern

## SS7 Security Issues.

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

# Issues of Concern

## SS7 Security Issues. > Solutions

| Protocol Forklift Upgrade | SS7 Hardening |
|---|---|
| Design new protocol with inherent security (authentication, encryption). | • optimal parameter configuration,<br>• logging<br>• examining of suspicious SS7 traffic<br>• firewalling based on<br>  • message type<br>  • source address |
| High complexity, Capital Intensive | |
| Participants : Vendors, Network operators, Regulators | |

# Issues of Concern

## Availability of Networks and Services.

| High Impact Outages | Low Impact Outages |
|---|---|
| Rare | Can be frequent and dispersed |
| Close attention by Providers | Providers keep to themselves |
| Close attention by Regulators | Regulators don't get Informed |
| Emphasis is given by relevant EU regulation (article 13a of Framework directive) | |
| Solutions are very carefully designed | Might be dealt with patchwork solutions |
| Good incident intelligence dissemination amongst telecom community | Need for better Incidence Intelligence dissemination (info quality, reporting) |

# Issues of Concern

## Availability of Networks and Services.

- ADAE consultation of required incidence intelligence that needs to be reported by CSPs.
  - Network area (i.e. access, aggregation, edge, core layers) that the incident occur,
  - Network systems (switch, router, BRAS, etc) that cause the incident and the system that is affected,
  - Geographical features of the affected area (i.e. island area or mainland),
  - Technical cause and effect of the incident,
  - Mean number of the affected subscribers.

# Issues of Concern

## Cross Border Cooperation.

- Multinational provider supervision by National Regulators is a challenge.
- Regulator Auditor personnel from one member state do not have the authority to travel across borders and audit the provider premises in another member state.
- The heterogeneous transposition of EU directives to the national regulatory and legal framework among the different EU member states also puts a further constraint.
- Regulator Authority cooperation provisions should be introduced in e-privacy & Network & Services Availability related EU directives & regulations as in the case of the General Data Protection Regulation 679/2016 (GDPR) .

# Issues of Concern

## Cloud Computing.

- Data retention paradigm where multiple CSPs share resources for storing communication data for legal investigation purposes allowing the possibility of a new service offering.
- Some reservations regarding true separation of such communication data amongst resource sharing CSPs.
- A concern exists, 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.

# Thank You for your Attention !!!

www.adae.gr

psallidasi@adae.gr