Managing Network-Level IoT Security and Privacy Risks with ANASTACIA

Adrian Quesada Rodriguez
MA, MSc. Lic. CIPP/E
Project Manager and DPO
Mandat International

IoT Week 2019
Aarhus, Denmark
The IoT Privacy/Security challenge

Internet of Things (IoT) connected devices installed base worldwide from 2015 to 2025 (in billions)

**GDPR principles** (art. 5)
- Lawfulness, fairness and transparency
- Purpose limitation
- Data minimization
- Accuracy
- Storage limitations
- Integrity and confidentiality

**Approach:**
Personal data protection and security by design and default (art. 25)

**Requirements:**
- Organizational: Consent and proof of consent, Underage consent, DPIA...
- Technical: Encryption, anonymization, access management...
- Administrative: Data breach reports to DPA

Who can solve the compliance puzzle?

Internet of Things (IoT) connected devices installed base worldwide from 2015 to 2025 (in billions)

How to enable Privacy/Security management for all?

IoT pervasivity: VALUE ADDED vs (ACCEPTED?) RISKS
ANASTACIA’s mission

- To develop a trustworthy-by-design autonomic security framework which will address all the phases of the ICT Systems Development Lifecycle (SDL) and will be able to take autonomous decisions through the use of new networking technologies such as Software Defined Networking (SDN) and Network Function Virtualisation (NFV) and intelligent and dynamic security enforcement and monitoring methodologies and tools.

- Holistic solution enabling trust and security by-design for Cyber Physical Systems (CPS) based on IoT and cloud architectures.
ANASTACIA framework

Security development paradigm

Distributed trust and security components and enablers

Holistic Dynamic Security and Privacy Seal (DSPS)

Self-protection capabilities

Self-healing capabilities

Self-repair capabilities

VALUE CHAIN
ANASTACIA’s Approach

• **Focus:**
  – network-level threats and network technologies (SDN/NFV)

• **Security:**
  – Trusted Security Orchestration in SDN/NFV-enabled IOT
  – Security monitoring: DPI/DNI
  – Automated Cognitive Reaction and Mitigation Components
    • **Security Risk Assessment:**
      – severity, asset importance, cost of mitigation
    • **Consequence prediction and prevention.**
      – IDS/DPS + behavioral engine
Security + Privacy: How to connect them?

1. **DSPS (GUI):** Meaningful and simple information for CISO/DPO

2. **Mapping of monitored security threats to network-level privacy risks:**
   - Risk 1, 2, 4: access, modification and deletion of personal data (malware, etc.)
   - Risk 3: lacking anonymization/encryption of information
   - Risk 5: intra-network monitoring (man in the middle)
   - Risk 6: external network monitoring (insecure communication channels)
   - Risk 7: data availability and downtime (DDoS)

3. **ISO-based privacy risk assessment process**

4. **CISO/DPO signed feedback + non-repudiable audit trail**
The Dynamic Security and Privacy Seal (DSPS) provides a holistic solution to privacy and security certification, addressing both the organizational and technical requirements enshrined by the GDPR.

DSPS is designed by:

- Combining conventional certification schemes with real-time dynamic monitoring
- Addressing the new European General Data Protection Regulation
- Modelling a secured and authenticated dynamic seal system as a service
The Dynamic Security and Privacy Seal (DSPS) provides a holistic solution to privacy and security certification, addressing both the organizational and technical requirements enshrined by the GDPR.

DSPS is designed by:
1. Combining conventional certification schemes with real-time dynamic monitoring
2. Addressing the new European General Data Protection Regulation
3. Modelling a secured and authenticated dynamic seal system as a service
**Dashboard**

**Current Seal**

Report

Is this alert relevant for personal data protection purposes?
Yes

Type of incident
Forbidden Network Authentication

Date of incident
June 12, 2019, 5:28:32 pm

Date of discovery
June 12, 2019, 5:28:36 pm

Cause of Incident
Excepteur sint occaecat cupidatat non proident

Assets involved
1. Ut enim ad minim veniam, 2. Itaque earum rerum

**Seal History**

<table>
<thead>
<tr>
<th>Seal</th>
<th>Cause</th>
<th>Date</th>
<th>Global Risk</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>🟢</td>
<td>Manually restored: see log for details.</td>
<td>Jun 14, 2019 5:38 pm</td>
<td>0</td>
<td>Get Log</td>
</tr>
<tr>
<td>🔴</td>
<td>Simulated alert: Forbidden Network Authentication</td>
<td>Jun 14, 2019 5:18 pm</td>
<td>10</td>
<td>Get Log</td>
</tr>
</tbody>
</table>

**DPIA**

Latest DPIA

DPIA. PDF
104.20 KB
EU Security/Privacy-compliant IoT Business Ecosystem
Take-aways

• Human-focused Privacy and Security by design is necessary to enable trust
• ANASTACIA can help track the implementation of these principles in IoT/CPS architectures
• The DSPS aims to bridge privacy and security perspectives in a trustworthy manner
Contacts

- **Project Coordinator**
  Stefano BIANCHI (Softeco Sismat)
  stefano.bianchi@softeco.it

- **Scientific and Technical Project Manager**
  Antonio SKARMETA (Universidad de Murcia)
  skarmeta@umu.es

- **DSPS Coordinator**
  Adrian QUESADA RODRIGUEZ (Mandat International)
  aquesada@mandint.org
ANASTACIA has received funding from the European Union’s Horizon 2020 Research and Innovation Programme under Grant Agreement N° 731558 and from the Swiss State Secretariat for Education, Research and Innovation.