Operational Security Assurance:  
“Requirements for a trusted future internet and privacy"

Bertrand Marquet  
Head of Security Research Dept (Acting)  
Alcatel-Lucent Bell Labs France
Agenda

- Introduction
- Operational Security Assurance
- Requirements for Security Assured Operations
- Assurance Profiles in operations
- Conclusion
Introduction
Several major transformation are occurring simultaneously

You will be here
Technological context: Telco is facing two major transformations

- Mastering risks of service infrastructures
  - ICT Cloud: Elastic Telco Cloud
  - ICT infrastructures: IT Cloud (virtualized resources)
- Transformation of infrastructures

- Protecting User experience: Privacy and usability
  - Internet of Things: Application stores
  - PCs, Smartphones: Application stores
- Transformation of End devices

- Service providers
- End users

- Transformation of End devices
Social and economical context

- New ecosystems
- Open Services and APIs
- Spikes in resources demand
- Need to comply with more and more regulations
- Social life exposed
- Open platforms
- Everything is Video
- Content provider
- Application provider

End users

Service providers
Operational Security assurance to provide guaranties

Mastering risks of service infrastructures

Protecting User experience Privacy

Operational Security Assurance Protecting Business and Privacy
Operational Security Assurance
Linked European projects

Part of this work has been studied within EUREKA Celtic Project

2005-2007: BUGYO - CELTIC Excellence award

2009-2011: BUGYO beyond
Large-scale, multi-domain and dynamic infrastructures

Content of the following slides cannot be used without Alcatel-Lucent
And BUGYO Beyond consortium written authorization
Between risk management and trust management:

**Assurance Management**

- **Metrics**
- **Measurement**
- **Evidence**
- **Assurance**

- **Risk Management**
- **Countermeasures**
- **Trust management**
- **Confidence**

- **Inclur**

---

Copyright © 2010 Alcatel-Lucent. All rights reserved.
Top down approach: From service to indicators.

- Inherent risks for the Service
- Identified risks for the Service
- Security Policy
- Security Architecture
- Security Controls realisation
- Running Security Controls

Procedures and Technical mechanisms enforcing or supporting security controls

Accepted risks

Implementation gap (CC evaluation scope)

Application gap (operational evaluation scope)
Methodology and tools

preparatory steps

operational steps

Service modeling   Metric selection   Measuring   Aggregation   Evaluation   Presentation

Learning process

continous
Requirements for Security Assured Operations
Assurance profile: a commonly agreed requirements

1. Service

2. Service infrastructure

3. Target of Measurement

4. Security Assurance Views

Copyright © 2010 Alcatel-Lucent. All rights reserved.
Assuranceprofilcontent
Leveraging expertises in a common formalized format
Associated method: From risk assessment to probes deployment
Defining Assurance profile
Step 1: identifying Security Problem
Step 3: From Compliance to security requirements

- List of Security Objectives from risks reduction
- Binding / coherence checking
- List of incoherence and remediation

AP_SSO: Service Security Objectives

AP_OSR: Object Security Requirements

List of identified security countermeasures

Part 1 SFR[ISO15408]
[ISO27001-ISO27011] (other standards to identity)

List of identified security countermeasures [ISO27005] 8.2.1.4
With new identified for risk reduction

List of standards/ regulations/ Policies/ Best practices

AP_CCL: Compliance Claim

Separation

List of Security Objectives and best practices from AP_CCL

AP_CCL: Compliance Claim

List of Measurement Objectives from AP_CCL

List of Security Objectives and best practices from AP_CCL

List of existing security countermeasures [ISO27005] 8.2.1.4
With new identified for risk reduction

List of identified security countermeasures

List of existing security countermeasures [ISO27005] 8.2.1.4
With new identified for risk reduction
Step 4: Deriving Object Measurement Requirements

List of Measurement Objectives from AP_CCL

AP_OSR:
Object Security Requirements

Identification of measurement objectives

List of Measurement Objectives from AP_OSR

Binding / coherence checking

List of incoherence's and remediation

AP_OMR:
Object Measurement Requirements

Measurement taxonomy (API | Standards)

3'

4

All requirements are expressed using Measurement taxonomy as a simple binary question:
In [taxonomy domain] of [Security countermeasures] on [TOM-object] is (running) as expected ?
Taxonomy domain = static-configuration, dynamic configuration, etc... (WP2 taxonomy)
Step 5: Defining Target of Measurement and assurance views

1. Identify view(s)
2. List of Views and objectives
3. Construct view(s)
4. Add Define SAVObject
5. AP_TOM: Target of Measurement
   - list of existing security counter measures
6. AP_SAV: Security Assurance Views
   - list of selected supporting assets
7. AP_OMR: Object Measurement Requirements
   - list of metrics

(AP) Views definition
Assurance profile in operations
Service infrastructure

Assurance Profile for this service

(TOM + SAVs)

Presentation

operational steps

Service modelling

Metric selection

Measuring

Aggregation

Evaluation

Presentation

preparatory steps

continuous

Learning process

Critical Infrastructure Objects

Security Assurance Views

Security Assurance Views

Target Of Measurement

Learning process
**APPLICABILITY and COMPLIANCE**

- **Applicability Requirements satisfied?**
  - **YES**
    - Use AP to deploy assurance program
  - **NO**
    - Use AP as support tool only but No compliance can be claimed

Specific service deployment

- Contract SLAs Certification Accreditation
- AP compliance (Objective level, Requirements level Views level)
Deriving assurance profiles into models and metrics
Binding profiles with infrastructures

Instantiation of deployed views and binding to measurement framework
Conclusion
Operational security assurance

- Both from service providers and end user privacy, security assurance can lead to trust as it
  - Requires formalized expression of security requirement
  - Requires formalized expression of security verification
  - Helps different entities of large organizations to communicate
  - Allow confidence in deployed security without having details of mechanisms deployed
    - Privacy aspects (guaranties of protection without revealing information)
    - Service level agreement based contracts
  - Allows best practices approach to extent to more formalized, comprehensive and coherent approach to security
    - From risk management to trust management