ITU-TRCSL Symposium on Cloud Computing
(28-30 July 2015 Colombo Sri Lanka)

Architecture, Management, Cloud Interoperability, Security

Dr. Ruan HE,
Senior Expert, Orange
ruan.he@orange.com
Outline

1. Cloud Functional Reference Architecture
2. Inter-Cloud and Cloud Management
1

Cloud Functional Reference Architecture
CCRA architectural views (Y.3502)

In scope

- User view
- Functional view
- Deployment view
- Implementation view
CCRA user view (activities)
CCRA functional view - functional architecture/ -components

User layer
- User function
- Business function
- Administrator function

Access layer
- Access control
- Connection management

Service layer
- Service capabilities
- Business capabilities
- Administration capabilities
- Service orchestration

Resource layer
- Resource abstraction and control
- Physical resources

Multi-layer functions
- Integration: Service integration
- Security systems: Security integration, Authentication and identity management
- Operational support systems: Service catalogue, Provisioning, Monitoring and reporting
- Business support systems: Account management, Subscription management
- Development support: Build management, Test management

User/ Functional View Relationship

User layer
- User function

Access layer
- Service access

Service layer
- Service capabilities

Resource layer
- Resource abstraction and control
- Physical resources

Multi-layer functions
- Integration
  - Service Integration
- Security systems
  - Authentication and identity management
- Operational support systems
  - Authorization and security policy management
- Business support systems
- Development support
Infrastructure as a Service (Y.3513)

- **computing service functions** allow CSC to provision and use processing resources.
- **storage service functions** allow CSC to use storage resources.
- **network service functions** allow CSC to use networking resources.
2

Inter-Cloud and Cloud Management
Inter Cloud Computing (Y.3511)
Multi Cloud Management
Inter Cloud Computing (Y.3511)
Security of Cloud Computing
## SG17 Structure

<table>
<thead>
<tr>
<th>WP1: Fundamental security</th>
<th>Q1: Telecommunication/ICT security coordination</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Q2: Security architecture and framework</td>
</tr>
<tr>
<td></td>
<td>Q3: Telecommunication information security management</td>
</tr>
<tr>
<td>WP2: Network and information security</td>
<td>Q4: Cybersecurity</td>
</tr>
<tr>
<td></td>
<td>Q5: Countering spam by technical means</td>
</tr>
<tr>
<td>WP3: Identity management and cloud computing security</td>
<td>Q8: Cloud computing security</td>
</tr>
<tr>
<td></td>
<td>Q10: Identity management architecture and mechanisms</td>
</tr>
<tr>
<td>WP4: Application security</td>
<td>Q6: Security aspects of ubiquitous telecommunication services</td>
</tr>
<tr>
<td></td>
<td>Q7: Secure application services</td>
</tr>
<tr>
<td></td>
<td>Q9: Telebiometrics</td>
</tr>
<tr>
<td>WP5: Formal languages</td>
<td>Q11: Generic technologies to support secure applications</td>
</tr>
<tr>
<td></td>
<td>Q12: Formal languages for telecommunication software and testing</td>
</tr>
<tr>
<td>Question</td>
<td>Date</td>
</tr>
<tr>
<td>----------</td>
<td>------</td>
</tr>
<tr>
<td>1. Security architecture/model and framework</td>
<td>Q3/17</td>
</tr>
<tr>
<td>2. Security management and audit technology</td>
<td>Q3/17</td>
</tr>
<tr>
<td>3. BCP/disaster recovery and storage security</td>
<td>Q3/17</td>
</tr>
<tr>
<td>4. Data and privacy protection</td>
<td>Q3/17</td>
</tr>
<tr>
<td>5. Account/identity management</td>
<td>Q3/17</td>
</tr>
<tr>
<td>6. Network monitoring and incidence response</td>
<td>Q4/17</td>
</tr>
<tr>
<td>7. Network security</td>
<td>Q4/17</td>
</tr>
<tr>
<td>8. Interoperability security</td>
<td>Q8/17</td>
</tr>
<tr>
<td>9. Service portability</td>
<td>Q8/17</td>
</tr>
</tbody>
</table>

Management | CyberSecurity | (Main)cloud | IdM/Bio

Cloud Security Work Items

X.1601: Security framework for cloud computing

X.cc-control: Information technology – Security techniques – Code of practice for information security controls for cloud computing services based on ISO/IEC 27002

X.sfcse: Security functional requirements for SaaS application environment

X.goscc: Guideline of operational security for cloud computing

X.Idmcc: Requirement of IdM in cloud computing

X.CSCdataSec: Guidelines for cloud service customer data security

Published in 2014.1
Common text with ISO/IEC
Established work item in 2014-09 SG17 meeting
Cloud Security Recommendations

Overview

X.1601: Security framework for cloud computing

Security design

X.1602-X.1605
Security requirements (e.g. X.sfcse), Security capabilities

X.1606-X.1610
Trust model
Security architecture/functions

X.1611-X.1615
Security controls (e.g. X.cc-control)

Security implementation

X.1616-X.1625
Security solutions
Security mechanisms

X.1626-X.1630
Incident management, disaster recovery
Security assessment and audit

Best practices and guidelines

X.1631-X.1640
Best practices / guidelines (e.g. X.goscc)
Conclusion

1. Cloud Functional Reference Architecture
   - Chart of functionalities and their dependency
   - Layers and transversal aspects

2. Inter-Cloud and Cloud Management
   - 3 modes of federation
   - Cross-management

   - major standard: X.1601
   - new standard: ISO/IEC JTC1 27017
Thank you!