China unicom中国联通
创新·改变世界

电信能力开放安全标准化研究

中国联通 网络技术研究院
高枫

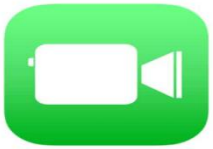
目录

电信运营商面临的挑战

China unicom中国联通 创新·改变世界

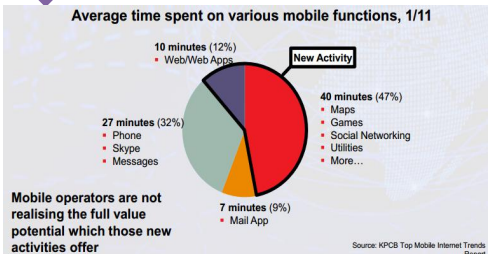
OTT迅猛发展

- 随着移动互联网的应用普及，互联网公司不断创新业务模式
- 迅速聚集数以亿计用户，提供丰富多彩的服务
- 突出特点
  - 用户粘性高
  - 应用创新性强
  - 覆盖面广等
- 创新型服务中，不乏足以替代电信运营商的业务形态
  - 苹果的iMessage 可替代传统的短彩信
  - 苹果Facetime可取代视频电话等




运营商增量不增收

互联网公司	•加快技术创新和产品部署 •形成取代传统运营商部分业务的趋势
用户	•移动通信技术不断发展，智能终端数量增长 •用户使用移动互联网应用产生的流量增速迅猛
电信运营商	•面临沦为只能提供网络获取流量费用的管道，即被管道化 •应用的附加利润由互联网公司获取，电信运营商面临着增量不增收的问题



亟待探索创新业务模式

遭受OTT业务最大冲击的是传统电信业的封闭、自我发展模式

随着OTT业务的发展，传统CP/SP合作伙伴的价值下降

以运营商为核心的产业链在解体，运营商对产业链的掌控能力在削弱

运营商亟待探索创新业务模式

能力开放，创新的业务模式
将数字资产开放变现的过程
缩小基础业务收入
开创新的收入来源

目录

运营商能力开放现状分析

电信运营商实践

国外运营商

- 美国
  - AT&T：为开发者开放API
- 欧洲
  - Vodafone：移动安全服务、移动支付
  - Orange：流量经营
  - 西班牙电信：开放平台、Web App、移动支付、移动金融

国内运营商

- 中国联通：Wo+，能力开放平台
- 中国移动：能力开放平台
- 中国电信：能力开放平台

运营商	开放战略	类别
AT&T	开放API，不仅可用于iOS、Android、Symbian等各智能手机的本地应用，还支持HTML5应用	API开放
Vodafone	与BAE系统公司联合研发企业安全解决方案；与Visa签署全球伙伴关系，开发以沃达丰为品牌的手机支付项目；推出VBP（Vodafone business place），为终端用户提供订购下载使用商务应用的平台，为开发者提供开发应用发布应用测试应用的工具，为能力开发者提供开发能力发布能力的渠道	移动安全服务 移动支付
法国电信Orange	与Google实现流量内容双向收费，Google向Orange支付的流量费用将用于维护网络，以确保用户能够快速访问Google的内容	流量经营
西班牙电信	打造BlueVia统一开放平台；与Mozilla合作推出首款基于开放互联网的HTML5标准设备平台；与万事达公司在拉美建立的移动金融解决方案合资企业，与Visa欧洲公司签署了包括移动钱包、NFC等在内的移动商务领域战略合作协议，与Facebook、谷歌、微软和RIM签署全球框架协议，联合提供手机账单支付服务	开放平台 Web APP 移动支付 移动金融
中国联通	发布Wo+开放战略，依托中国联通的业务平台，将互联网的应用服务资源快捷方便地呈现给用户。能力共享平台提供短信、彩信、语音、IVR、统一帐号以及云通讯录等能力调用，同时汇聚互联网各类资源，输出给应用提供商	能力开放平台
中国电信	建设综合业务接入网关（ISAG）与综合业务管理平台（ISMP）实现对业务能力的开放和管理，并建设中国电信天翼开放平台汇聚中国电信八大互联网基地两大专业公司及增值业务运营中心的大多数内容和信息能力，所有能力以标准互联网API接口形式面向合作伙伴统一开放	能力开放平台
中国移动	增值业务综合运营平台（VGOP）建设上，从流程、功能、数据接口等几个方面全方位推动增值业务从孤立走向整合	能力开放平台

目录

能力开放安全标准研究

China unicom中国联通
创新·改变世界

能力开放需保障安全

创新业务模式
- 能力开放，新的业务模式
- 有助于运营商与ISP获得双赢

核心业务
- 运营商的核心业务能力
- 电信服务能力应安全的开放
- 全方位的保护

安全威胁
- 来自第三方的不安全或恶意的应用服务
- 可能将对运营商的业务系统、传输网、用户信息等带来威胁

相关标准组织工作

国际标准组织
- ITU-T
- 3GPP
- GSMA
- OMA

国内标准组织
- CCSA

ITU 3GPP A GLOBAL INITIATIVE GSMA IETF oma Open Mobile Alliance 中国通信标准化协会 China Communications Standards Association

能力开放安全标准研究

China unicom中国联通
创新·改变世界

ITU-T
- ITU-T SG 17 Q7已开展相关标准研究
- 电信服务能力开放的安全需求和框架
- Security framework and requirements for open capabilities of telecommunication services

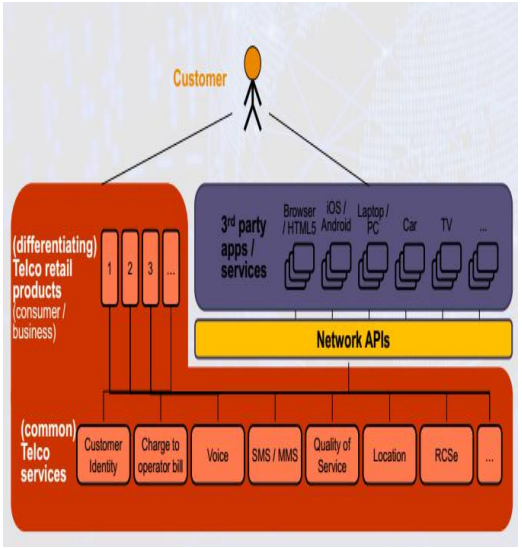
3GPP
- Parlay X ：开放业务架构规范
- 需求组SA1: Service Exposure and Enablement Support (SEES) requirement study
- 架构组SA2: Architecture enhancement work for service capability （AESE）
- 安全组SA3：AESE Security

GSMA
- OneAPI：业务能力开放标准方面制定
- 为移动运营商定义一套通用的轻量级、友好型网络接口
- 便于互联网厂商以及其他应用开发商甚至个人开发者能够更轻松地获得移动运营商的网络能力
- 安全机制：认证

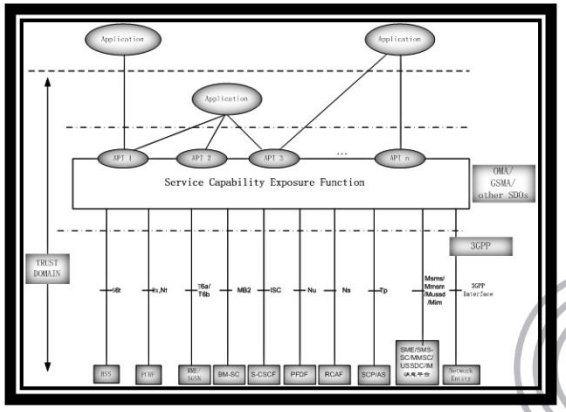
IETF
- OAuth 2.0
- 用于验证和授权的标准
- 定义四种获取访问令牌的方式

OMA
- OAuth 4.0
- OMA的OAuth4 API工作组以OAuth2为基础，研究
  用户将其拥有的网络资源通过业务能力开放平台授权给第三方应用的一种认证授权架构

CCSA
- TC5WG9
- 面向应用能力开放的移动数据网络总体技术要求
- 安全要求：能力开放平台与可信任域其他网元之间的安全机制；能力开放平台与第三方应用之间的安全机制



网络API



能力开放平台系统架构

ITU
3GPP A GLOBAL INITIATIVE
GSMA
IETF
oma Open Mobile Alliance
中国通信标准化协会 China Communications Standards Association

ITU-T X.1145 （1）

China unicom中国联通
创新·改变世界

电信服务能力开放的安全需求和框架

- 中国联通牵头在ITU-T SG17 Q7 立项
- “电信服务能力开放的安全需求和框架”
- “Security framework and requirements for open capabilities of telecommunication services”

- 历时2年多的研究，目前已通过AAP流程，作为ITU-T X.1145标准发布

AAP Recommendation: X.1145

Work Programme:X.1145

Basic Information

Title	Study Group	Current Status	Consent Date	Approval Date	Study Period	Provisional Name	IPR	Input used for Consent
Security framework and requirements for open capabilities of telecommunication services	17	A	2017-03-30	2017-05-14	2017-2020	X.websec-6	?	TD 0298 Rev.2

Observation

AAP Process Details

Last Call (LC)				Additional Review (AR)				Study Group (SG)	
LC Start	LC End	LC Result	LJ Result	AR Start	AR End	AR Result	AJ Result	SG Date	SG Result
2017-04-16	2017-05-13	A							
[AAP-10]		[AAP-12]							
LC - Text / Summary				AR - Text / Summary				SG Documents	
LC Text LC Summary									
LC - Comments				AR - Comments				SG Decisions	

ITU-T X.1145 （2）

China unicom中国联通 创新·改变世界

通用模型

安全威胁 | 安全需求 | 安全功能

■分析电信能力开放面临的安全威胁

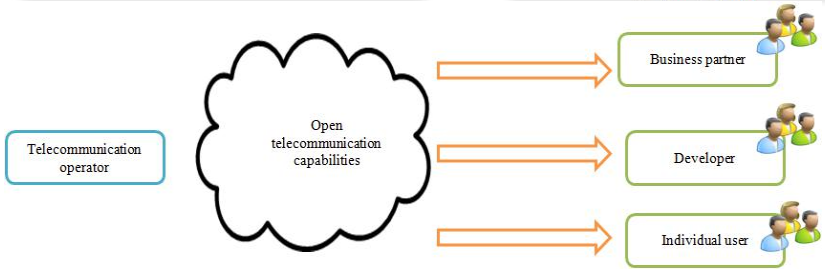
- 修改开放的能力
- 非授权的访问
- 木马和病毒攻击
- 泄露个人信息

■分析电信能力开放的安全需求

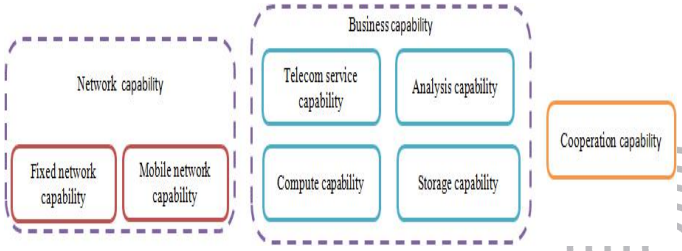
- 访问控制
- 认证
- 业务隔离
- DDoS/病毒的应急响应
- 创新业务上线前的安全测试
- 个人信息保护
- 物理网络安全
- 虚拟网络安全
- 安全审计

■ 根据安全威胁和安全需求分析，提出电信能力开放应提供的安全功能

- 访问控制
- 认证
- 数字签名
- 加密
- 事件监测
- 密钥交换
- 安全审计
- 安全恢复



通用模型



开放能力

ITU-T X.1145 （3）

China unicom中国联通
创新·改变世界

Threats / Entities	Unauthorized access	Modification of capability usage	Trojan/virus	Disclosure of personally identifiable information (PII)
Telecommunication operator	Y	Y	Y	Y
Business partner			Y	
The developer			Y	
Individual user			Y	Y
Entity between telecommunication operator and the business partner	Y	Y	Y	Y
Entity between telecommunication operator and the developer	Y	Y	Y	Y
Entity between telecommunication operator and the individual user	Y	Y	Y	Y

安全威胁与通用模型的关系

Functions / Requirements	Encipherment	Key exchange	Digital signature	Access control	Authen-tication exchanges	Event detection	Security audit trail	Security recovery
Business isolation	√	√		√				
Access control				√	√			
Authentication	√	√	√		√			
Secure audit							√	
Emergency response for virus/DDoS						√		√
Innovation business security test before online						√		
Physical network capability security				√			√	√
Virtual network capability security				√			√	√
Personally identifiable information protection	√	√	√	√	√			

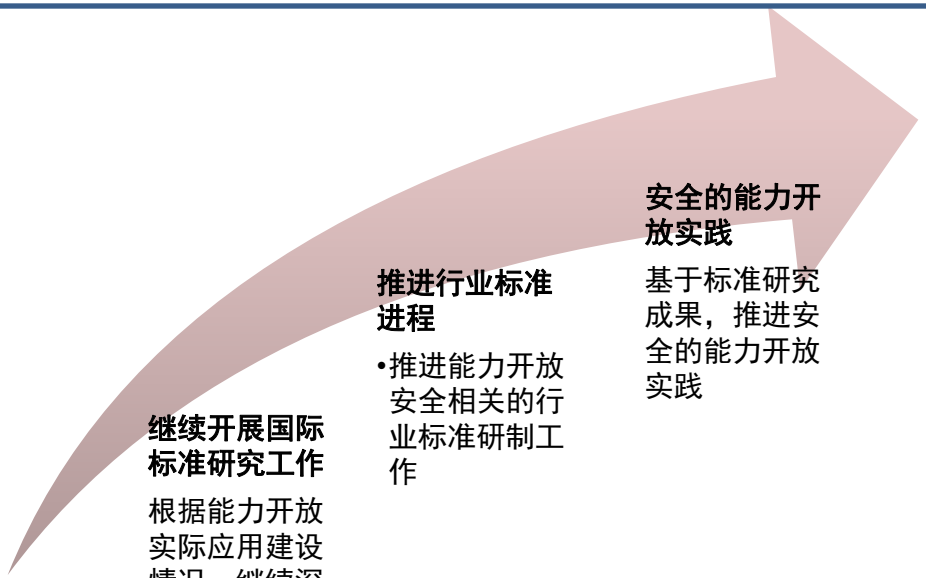
安全需求与安全功能的关系

目录

总结及展望

总结

- 随着OTT的迅猛发展，运营商亟待寻求新的业务创新模式以解决增量不增收的问题
- 电信业务能力开放作为一种新的业务模式有助于运营商与ISP获得双赢
- 作为运营商的核心业务能力，电信服务能力应安全的开放并对其进行全方位的保护
- 研究电信服务能力开放的安全框架和全面分析其安全需求，能够解决能力开放面临的安全问题，确保电信服务能力开放业务的安全运行
- 通过标准的研究
  - 可以引导产业界运营商及互联网服务提供商开展电信服务能力开放相关业务安全的研究
  - 促进研究的深入开展以及引导产业安全、良性发展
  - 指导运营商及互联网服务提供商安全开展新业务并有助于业务应用落地



China unicom中国联通
创新·改变世界

谢　　谢　　！

China unicom中国联通
创新·改变世界

电信能力开放安全标准化研究

中国联通 网络技术研究院