5G广播视音频业务安全标准组提案

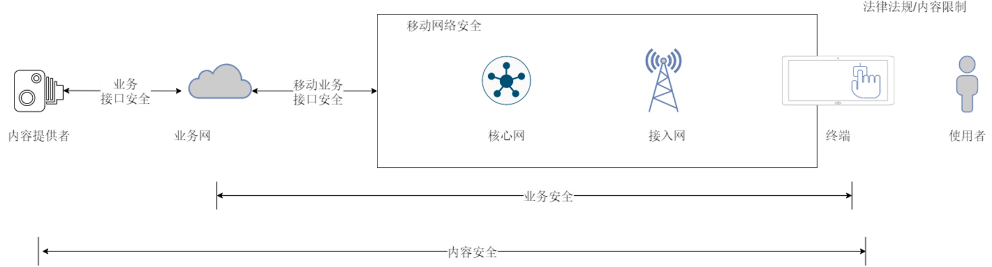
标准组：02-5G广播视音频业务安全

单位：高通无线通信技术（中国）有限公司

提案名称：安全需求与风险分析

1 简介

本提案分析了5G广播视音频业务安全需求与安全风险，基于此分析可展开业务安全解决方案及安全措施的设计。

本提案基于的基本系统架构如下：

上述架构仅为便于理解，不作为正文部分。

2 提案内容

* 与安全相关的业务场景分析

根据网络通信能力，终端可使用的服务分为3种类型，安全能力必须基于这3种类型进行设计：

1. 仅有接收5G广播信号的能力，不具备任何上行通信能力
2. 接收5G广播信号能力，且可与业务提供者进行IP双向连接，但不接入提供广播的无线网络
3. 接收5G广播信号能力，可与业务提供者进行IP双向连接，且接入5G蜂窝网络且可使用5G网络管理及安全保护和管理机制

根据终端对业务的处理能力，分为2种类型：

1. 可处理所有广播数据类型，包括媒体、消息和数据
2. 仅处理上述类型中的某个单一类型数据

根据终端的形态，分为2种类型：

1. 富智能终端： 丰富的用户（G）UI接口，开放的系统，可安装和管理软件
2. 专用终端： 无GUI接口，不可安装和管理软件

* 安全保护对象

在业务层面，5G广播系统涉及的安全保护对象包括：

1. 内容安全： 包括内容的完整性，合法性，以及内容是否合规，符合行业、区域等限制。内容是本业务的核心业务目标，防止内容播出被劫持是安全防护的核心。对内容的攻击可能来自对各个网络节点的数据替换，网络通信攻击（中间人/伪冒，篡改等）或直接在空口上进行伪基站广播。
2. 版权保护： 媒体在版权保护系统下传播、播放。
3. 认证： 广播服务提供者可信，可信终端认证。
4. 授权： 广播服务提供者在授权范围内发放数据；终端被合法授权，在授权范围内接收、使用数据。
5. 通信安全： 通信机密性（视场景和服务而定），完整性，来源可追溯；具有跨地域和时间的不可重放保护。由此可能要求系统有时钟的安全性要求，即系统中的分发节点和接收节点可能需要安全、可信的时钟信息。
6. 用户安全： 个人信息安全，未成年人保护。
7. 计费： 用户被正确计费，包括内容计费和网络计费。其中，用户不能借用免费服务进行非授权范围内的业务。

在基础设施和使能层，5G广播系统涉及的安全保护对象包括：

1. 网络通信服务及能力
2. 网络存储服务及能力
3. 数据和信息处理服务及能力

* 攻击

从攻击位置区分，攻击对象可能为：

1. 主机或节点处理： 内容提供者，服务提供者，无线网络节点，终端
2. 通信： 上述各点间的通信
3. 存储： 各节点的存储

从攻击类型区分：

1. 内容合规： 符合国家法律法规及管理要求
2. 伪冒： 伪冒内容源，业务播放节点，无线网络，终端，用户
3. 篡改： 各节点的处理或存储被篡改，网络通信中间人篡改
4. 泄露： 存储、通信被泄露，特别的，在终端进行媒体录制，二次传播
5. 提权： 各节点提权，网络使用特权提升（利用免费服务传播流量），播放超越版权限制媒体
6. 拒绝服务： 对源节点，节点进行DOS攻击；对网络通信进行DOS攻击；使用业务源端对网络或终端进行DOS攻击，使用网络对业务源端或终端进行DOS攻击；使用终端对网络或业务服务进行DDOS攻击。

* 风险分析

以上安全保护对象遭受攻击时，可能有以下风险：

1. 非法内容送达用户
2. 用户使用授权以外的服务
3. 媒体被违反版权保护传播
4. 网络服务被恶意使用
5. 网络及终端的正常服务遭受破坏
6. 用户计费错误，网络或用户遭受经济损失
7. 用户个人信息被非法处理或使用

* 广播系统特有的安全特征

仅考虑下行单向广播业务，安全性方面与一般的单播或组播业务流相比，有如下特征：

1. 广播信道，任何人可以发，发送端易被伪冒。尤其是在无广播网络覆盖或信号较弱的地区，伪冒的无线广播发送节点（例如伪基站）对用户分发。通过对内容、数据或网络的可选鉴别，对通信的防重放保护进行保护。
2. 广播信道，所有人收到的数据相同。如果使用单纯的对称密码技术进行完整性保护或加密（作为访问控制技术），则所有人使用的密码是相同的。而密码在播放器端可能被获取。被获取后，容易伪冒和访问控制失败。
3. 无法根据业务和终端能力进行安全配置和安全协商，端到端的安全措施与软硬件配置最低端的终端对齐。
4. 安全管理困难。根据场景分析，终端可能没有上行对网络或业务提供端的反馈通道，因此进行管理配置、升级更新有困难。

* 安全假设
  1. 终端攻击者

1. 攻击者可以具有合法访问服务和网络的账户及授权。
2. 攻击者可能与被攻击者地理位置接近，可以与被攻击者设备进行单向或双向无线通信。
3. 攻击者对其所持有终端有完全控制权，即攻击者可能在终端进行软件或部分硬件的通信数据分析、内存数据分析与伪造、修改编解码码及通信协议软件等能力。攻击者也可能通过屏幕与声音录制等方法获取视频、文字、图像。
4. 攻击者对其使用的IP网络访问有完整的控制权，即攻击者可以截断、窃听、重放、伪造网络通信数据，可以进行任何中间人攻击，包括对攻击者自身的及同一子网下的其他用户。
5. 若音视频是通过接口播放到媒体播放设备（例如通过HDMI，DP2，VGA等接口），则所有接口数据可以被攻击者获取、伪造、篡改等。
   1. 网络攻击者
      1. 攻击者可以有公共互联网的完全访问能力
      2. 内部攻击者（可能）对私有网络和基础设施有受控的访问能力

* 安全管理与审计

安全管理与审计包括对系统各节点基础设施、各节点间的通信要具备安全配置管理和事件、行为的记录能力。不同的部署场景下有不同的管理方式，例如业务网与移动网可能统一管理（属于同一个运营商）或分别管理（属于不同的运营商）。所有涉及节点和节点间的通信，使用安全记录和事后审计甚至即时处理，进行攻击溯源。

考虑到终端的能力及安全部署管理能力，可以考虑不同的安全目标和安全实现方式。例如，内容、业务、网络可能对内容进行完整性保护，但终端由于能力限制可能不做完整性校验直接播出。即便在此种情况下，终端也应具备一定的记录能力以供回溯使用。

* 信任与传递

若采用内容源或业务网与播放终端间的安全保护机制（机密/完整性保护），则需要在两端（终端/源端）配置部署信任关系。这种实现方式下，移动网络可仅作为传输的承载而不增加移动网络节点（BM-SC，GW，MME，eNodeB等）与UE间部署单独的保护机制（机密性/完整性保护）。这种实现方式下信任简单，无需传递。但在所有终端上配置信任凭据会带来管理的困难。

若采用分段部署的安全保护机制，即内容与业务，业务与无线网络间的接口，以及内部接口间进行安全保护，则可以利用终端对网络的信任（通过SIM卡或运营商配置），无需单独配置终端对业务网络的安全信任关系，相当于通过各个接口间的信任，将内容/业务提供者与终端间的信任传递到无线接入网。

3 结论

本提案对5G广播业务安全进行了系统性的基本分析，可作为进一步的安全需求分析和安全方案设计的基础和框架。

4 参考文献

注：

1、提案由标准组参与单位撰写提交。

2、提案编号为“WP-D9（该文档顺序编号，表示“提案”，此编号固定不变）-NN（标准组编号，2位）-SS（提案编号，2位）- vXXx（版本号，3位，表示第XX.x版本）”，比如“11”号标准组第7提案第“v020”版本的文件编号为“WP-D9-11-07-v020”。

4、提案行文标准：

1）提案统一采用A4纸，上下边距2.54厘米，左右边距2.8厘米；

2）页眉1.5厘米，页眉采用宋体，五号，左侧为文件编号，中间为文件名，右侧为文件完成时间；

3）页脚1.75厘米，页码采用宋体，五号，居中；

4）标题“XXX专题组提案”采用黑体，四号，居中排列，2倍行距；

5）节标题采用宋体，四号，1.5倍行距；

6）正文中文采用宋体，英文采用“Times New Roman”，小四，单倍行距；

7）正文中的图题和表题采用宋体，五号，居中排列。