DOI:10.3969/j.issn.1009-6868.2017.02.013
网络出版地址:http://kns.cnki.net/kcms/detail/34.1228.TN.20170302.1654.008.html

新一代视频业务安全解决方案

A New Generation of Video Service Security Solutions

中图分类号:TN929.5 文献标志码:A 文章编号:1009-6868 (2017) 02-0056-004

摘要: 视频业务互联网化给视频系统的存储、传输、内容属性、应用等各环节带来了相应的信息安全风险。分析了传统视频业务安全方案的不足,并提出了新一代视频业务安全解决方案,从根本上提升了视频业务的系统安全性和内容安全性,有效解决了视频业务运营所面临的安全问题。此外,还展望了视频业务安全的未来研究方向。

关键词: 视频业务;安全运维;防篡改;安全云;图像识别

Abstract: Internet-based video service brings information security risk to each part in the system, such as storage, transmission, content properties and applications. In this paper, the disadvantages of traditional solutions are analyzed, and a new generation of video service security solutions is proposed. In this way, system safety and content safety are enhanced, and safety problems of video business operation are solved. Moreover, the future research directions of video service security are also pointed out.

Key words: video service; security operation; tamper proofing; security cloud; image recognition

华新海/HUA Xinhai
贺镇海/HE Zhenhai
刘志军/LIU Zhijun
(中兴通讯股份有限公司,江苏 南京 210012)
(ZTE Corporation, Nanjing 210012, China)

1 视频业务安全解决方案概述

随着宽带网络和移动互联网的发展以及信息技术(IT)的进步,视频业务发展迅猛,其流量占据了网络流量的70%以上,已经成为继语音、短信、数据之后主要的电信基础业务[1]。据预测,移动视频流量在未来6年将增长24倍,2020年视频流量在网络数据消费的占比将会超过95%[2]。人们可以随时随地播放、下载视频,视频业务成为人们生活的重要组成部分。

视频业务的高速发展也给视频业务运营带来了严重的安全风险:

(1)互联网化的视频业务必然带来互联网化的主机分布式部署,其中的能力设备服务于公众,往往数量巨大,其安全管理和运维存在较大风险,每一个设计或运维缺陷产生的安全风险都会导致严重后果。

(2)如果播放内容的存储设备遭到黑客入侵并篡改,将迅速传播并在公众舆论中造成恶劣影响,给业务的运营商带来不可挽回的重大损失。

(3)视频业务往往具有强大的主机服务性能和网络带宽。如果这些主机或网络设备被黑客攻陷并植入后门,作为僵尸网络的一部分通过发起分布式拒绝服务(DDoS)去攻击其他服务,形成对互联网环境的"反噬",其危害无疑是巨大的。

(4)此外,缓存视频和其他类型资源的内容分发网络(CDN)作为资源加速设施,极大地节省了带宽,提升了用户体验。但由于源站可能存在不良资源(病毒文件,违反法律或公序良俗的图片、视频等),使得CDN系统存储并传播了这些内容,同样会导致不良影响并造成运营风险。

因此视频业务安全解决方案对于保障视频业务的运营极为重要。

2 传统视频业务安全方案及其不足

传统视频业务安全解决方案是参照传统基础电信业务安全解决方案来构建的。传统的基础电信业务从网络层、系统层、应用层等方面实施安全策略:

(1)通过对组网实施安全域划分,将各类网元划分为Trust、DMZ、Un-Trust等区域,对不同等级区域实施不同的安全策略,尽可能在安全性、服务性能等要素间取得平衡。

(2)对系统和数据设备实施安全加固,包括安全补丁的安装、合规配置、最小化服务、访问控制设置等。

(3)通过定期安全扫描、渗透测试等强化系统的安全评估,通过安全开发流程避免应用层漏洞。

上述基础手段有效地提升了系

收稿日期:2016-12-17
网络出版日期:2017-03-02

统安全性，降低系统被入侵的风险，但对视频业务而言仍然存在如下不足和风险：

（1）对视频业务中大量分布式主机安全管理能力不足。由于视频业务往往主机数量巨大且分布多个地市，某一个点出现某种安全弱点都有可能造成不良后果。

（2）对入侵行为响应缓慢，无法有效监测控制、阻止、告警。

（3）无法对视频业务中直播、点播的码流实施有效监测控制，防止码流在传输时被篡改造成恶劣影响。

（4）无法对设备中缓存的视频、海报模板等内容实施安全监管，尤其互联网应用服务（OTT）视频业务中的播放素材可能来源于不同的内容提供商甚至个人用户，其合法性需要得到快速有效地鉴别。

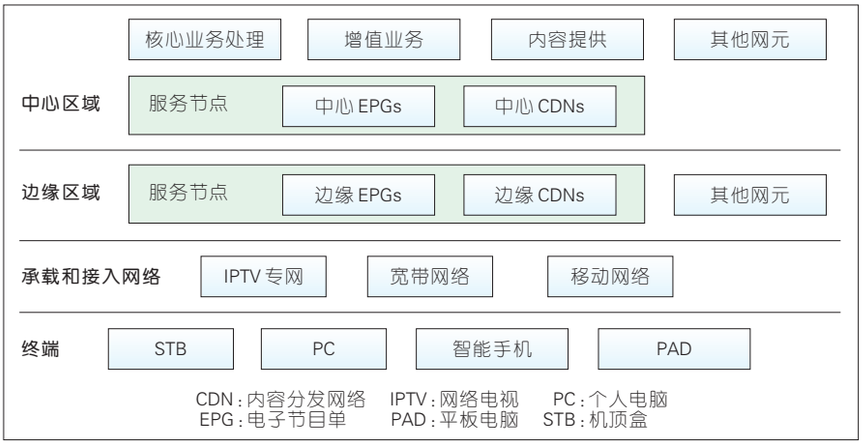
针对上述问题，我们提出了新一代视频业务的安全解决方案。

3 新一代视频业务安全解决方案

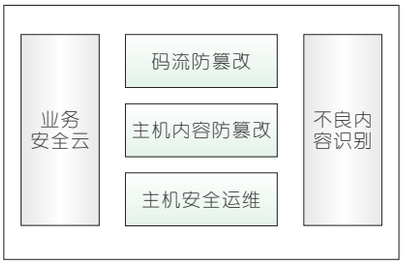
视频业务一般性的组网分层架构如图1所示，其中机顶盒、智能手机等终端通过宽带、移动网络等承载网接入到边缘服务节点，完成认证并向用户提供视频业务；边缘节点和中心区域的网元进行交互，实现如内容注入等业务流程。

相应的业务安全解决方案体系结构如图2所示。其中，各主要组成部分为：

- 主机安全运维——对视频业务大量的服务节点和中心节点，从日志管理、入侵检测、合规管理等方面提升系统基础安全性。
- 主机内容防篡改——在主机内核部署模块只允许指定进程对指定目录进行写操作，其他非法进程的写操作则直接被阻断并告警。
- 码流防篡改——通过数字签名方式检测视频流端到端的传输是否发生非法篡改。
- 业务安全云——对服务节点可能面临的Web攻击、DDoS攻击等安全威胁实施保护。
- 内容安全（不良内容识别）——对缓存在服务节点的视频、图片、文本等内容实施扫描，识别其中的不良内容（如黄色、暴力等）以及可能携带的系统病毒，通知业务系统采取进一步处置措施。



▲图1 视频业务逻辑架构



▲图2 视频业务安全解决方案体系结构

3.1 主机安全运维

视频业务往往需要在业务开展的地、市区域部署大量服务节点和若干中心节点。如前所述，大量的设备需要统一进行安全管理，避免因某个节点安全缺陷造成的风险。如图3所示，这里引入了主机安全运维方案，从进程管理、日志管理、设备管理、安全合规管理等几个方面提升视频业务节点的安全性。

（1）进程和账号管理：监测控制主机进程和账号，如果出现异常变化，如新增非系统以及非业务的进程和账号，立即生成日志并告警上报；

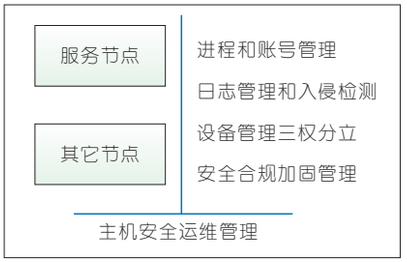
（2）日志管理和入侵检测：统一存储所有设备的日志信息，防止设备日志被非法删除或篡改，并分析日志信息，发现入侵痕迹及时告警上报；

（3）设备管理三权分立：将主机管理权限设置为管理员、操作员和审计员。

- 管理员包干管理若干节点主机并分配操作员，为其创建临时运维账号和操作时间窗，但管理员无操作设备权限；
- 操作员在指定的时间窗口进行运维操作，超出时间则其账号将被收回；
- 审计员审计设备操作状态，发现并处置安全隐患。

（4）安全合规加固管理：定期检测系统的合规配置，将不合规部分予以告警上报。

通过这4个方面的安全运维管理，节点安全状况从出现安全事件后被动采取措施，转变为事前主动检测、事中告警阻断和事后回溯，有效



▲图3 主机安全运维功能示意

提升了视频服务节点安全管控能力。

3.2 主机内容防篡改

如上文所述，服务节点内容被恶意篡改后的传播将导致恶劣的后果。传统的防篡改方案基于比对，设定可信源后，定期将目标目录下的文件和可信源依次比对。该方案的问题在于：

（1）比对过程极大消耗了系统资源，且视频业务中服务节点分布各地，数量众多，需要保持数据同步；

（2）如果可信源被攻破，则后续的比对都将失去意义；

（3）比对周期之间如果发生篡改，则非法篡改的内容依然会被迅速传播，导致方案失效。

新一代主机内容防篡改方案在电子节目单（EPG）、CDN等服务节点部署基于内核的防篡改模块，针对存储的内容文件，依据预先配置的策略，只允许合法进程对相应目录写操作，其他进程均视为非法，并禁止增加、删除、修改这些目录下的文件。

对应的策略配置形如：

目录1——进程1

目录1——进程2

目录2——进程3

……

其含义为对目录1，进程1和进程2可做写操作（如EPG模板更新、CDN内容注入等）；对目录2，进程3可做写操作。其他进程对目录1、2的写操作将被直接阻止，同时做告警操作。

对应于传统比对方案，该方案的优势在于：

（1）基于内核驱动模块，执行过程对性能消耗几乎可忽略不计；

（2）不需要设置可信源以及基于可信源的数据同步；

（3）发生的篡改被直接阻断，不留下任何传播恶意信息的时间窗口。

3.3 端到端的码流防篡改

互联网环境下，提供视频业务的节点直接面向公众传送视频流。为防止码流在传输到终端的过程中被非法篡改，造成用户无法收看正常的节目甚至接收恶意码流，造成不良影响，引入端到端的码流防篡改方案。

（1）在视频源的后向增加签名服务器，接收视频流，根据加密算法生成签名信息流；

（2）如果终端具有鉴别签名信息流能力，则同时接受来自CDN节点的视频流和来自签名服务器的签名流，并对视频流计算签名值和签名流比对，如一致则接收到的视频流合法，否则该视频流非法，进行阻断和告警处理；

（3）如果终端不具备鉴别签名信息流的能力，则在CDN节点之后，视频流接收终端之前的位置部署签名检测服务器，进行上述的类似检测和告警。

采用如上的带外方式和节点并行部署签名服务器，在不改变现有组网的情况下，有效保证了端到端的码流传输安全。

3.4 业务安全云

提供互联网视频服务的节点可能面临的攻击包括Web应用层攻击、系统级0day攻击、DDoS攻击等。上文已提及基础的安全加固、安全开发流程可一定程度缓解这些攻击，但仍取决于系统研发人员和工程人员的安全意识和能力。

新一代视频业务安全解决方案包括了业务安全云方案，在业务服务节点前置安全云，根据服务节点的特点搭载可选的Web应用防火墙、抗DDoS、定制抗特定0day漏洞、文件病毒扫描等功能，其架构如图4所示。

（1）抗DDoS模块可选用轻量级的基于规则的异常流量探测和实时阻断方案，或者重量级的流量清洗和回注方案；

（2）针对服务节点中的EPG等Web应用防护，架设Web应用防火墙，抵御常见的Web攻击；同时针对突发的0day漏洞，且后向服务节点无法及时升级补丁的场景，提供虚拟补丁引擎，针对漏洞特点编写规则，以防火墙方式抵御入侵；

（3）如果服务节点和客户端发生文件传输，则在传输过程中可以通过安全云实施病毒扫描，以阻止病毒文件的扩散。

业务安全云服务的具体部署特性如下：

（1）根据后向服务节点情况配置上述何种防护措施，如针对互联网缓存系统可配置上述3种安全功能，针对EPG配置Web应用防火墙（WAF）&虚拟补丁以及轻量级的抗DDoS功能等；

（2）根据服务节点传输流量线性调整安全云服务的部署，配置足够且可靠的安全服务能力，且不会因为其单点故障导致整个服务失败。

3.5 内容安全

以上章节探讨了视频业务设备节点针对黑客攻击的防御方案，可以归结为系统安全问题。另一方面节点存储的内容来源也会随着业务发展而日趋多样化，如多家内容提供商甚至个人用户上传的自制视频内容等。尽管视频服务运营商未必直接生产内容，但仍要对其存储内容的合法性负有相应的责任。因此，需要一套高效可行的解决方案来鉴别视频业务存储内容的合法性，也就是内容安全问题。

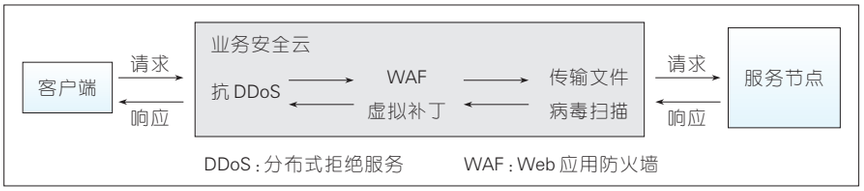
不良内容的识别可针对图像和视频，如图5所示，处理流程可分为如下步骤：

（1）服务节点下发文件采集策略，告知新增了哪些待判别的文件；

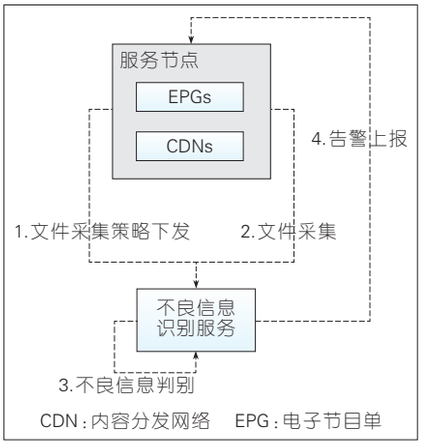
（2）根据策略向服务节点采集待判别文件并存储在本地；

（3）对采集的视频、图像等资源实施判别；

（4）将判别出的不良文件信息上报到服务节点，待后者进一步处置，处置方式则包括文件删除、通知管理



▲图4 业务安全云架构示意



▲图5 视频服务节点内容安全示意

员、记录日志、降低源站信用等级等。

不良信息的判别采用基于大数据的机器学习方式。对图像的判别分为离线、在线两个阶段[3]。

（1）离线：采集数十万张以上的正负样本，提取图像特征值并入库；

（2）在线：获得待判别的目标图像，提取特征数据，并依据上述特征值，利用机器学习算法判断目标图像非法的概率，概率大于一定阈值则判定为非法[4-5]。

不良图片的判别准确率一方面依靠机器学习算法的选型和实现，另一方面则有赖于离线阶段样本的收集。此外，图形处理器（GPU）运算技术的运用将大幅提升离线和在线运算的效率。

视频文件的鉴别可通过抽帧方式转化为图片，再利用上述图片判别方式进行判别。

4 视频业务安全未来研究展望

随着视频业务的不断发展，视频业务安全研究的新课题也将不断涌现。从目前来看，未来视频业务安全研究将有如下两方面的重要内容。

一方面是对视频内容安全实时监测控制技术的研究。现有方案将视频文件抽帧得到图片实施判断，如果图片采样率过高会消耗大量计算资源，采样率过低则判断精确度下降。随着人工智能和机器学习的发展，未来针对视频画面、声音的具体内容以及前后帧关联，需要提出更加高效的实时算法去判断视频内容合法性，从根本上解决流媒体内容安全问题，确保视频平台作为社会传媒核心系统的安全性，避免造成不良的社会和政治影响。

另一方面是大数据分析平台在视频业务安全中的应用研究。将网络设备、主机、应用、安全设备等产生的所有网络行为数据（含日志、流量等）进行收集，结合内部基础信息，包括资产、组织架构、人员账号、安全域等上下文信息，构建核心大数据分析算法模型，对复杂的网络攻击事件和内部违规行为进行深度挖掘，考量网络、主机、应用、数据等各条安全防护措施[6]，度量视频业务网络安全一般状况，同时预测业务安全潜在的安全攻击等风险，及时发现现有视频业务网络及平台安全解决方案所存在的问题，并提醒运维人员在哪一环节存在短板需要弥补[7-8]。

5 结束语

通过上述分析可知，对视频业务而言，单一维度的安全防护措施无法全面解决安全风险，整个安全防御体系中任何一个点出现偏差都有可能功亏一篑。因此，我们只有从系统、存储、传输、攻防手段、内容属性等多个维度建立视频业务的完整安全防护体系，才能从根本上解决互联网环境下视频业务的安全问题。

参考文献

[1] 曹珈, 徐火顺, 尹芹. 大视频变革之路[J]. 中兴通讯技术(简讯), 2016, (3):19-23
[2] 华新海, 刘耀东, 徐火顺. 下一代融合视频业务架构与演进[J]. 电信科学, 2015, 31(4):2-9. DOI: 10.11959/j.issn.1000-0801.2015094
[3] 陈骁, 金鑫, 谭晓阳. 基于躯干检测的单人不良图片识别[J]. 中国图象图形学报, 2016, 21(3): 348-355. DOI: 10.11834/jig.20160309
[4] LIU Y, LIN S, SHENG T, et al. Adult Image Detection Combining BoVW Based on Region of Interest and Color Moments[C]// IIP 2010:Intelligent Information Processing V, Uk:DBLP, 2010:316-325. DOI: 10.1007/978-3-642-16327-2_38
[5] YAN C C, LIU Y, XIE H, et al. Extracting Salient Region for Pornographic Image Detection[J]. Journal of Visual Communication & Image Representation, 2014, 25(5):1130-1135. DOI:10.1016/j.jvcir.2014.03.005
[6] 杨曦, GUL J, 罗平. 云时代下的大数据安全技术[J]. 中兴通讯技术, 2016, 22(1):14-18. DOI: 10.3969/j.issn.1009-6868.2016.01.004
[7] CARDENAS A, MANADHAT P, RAJAN S. Big Data Analytics for Security[J]. IEEE Security & Privacy Magazine, 2013, 11(6):74-76. DOI: 10.1109/MSP.2013.138
[8] XU L, JIANG C, WANG J, et al. Information Security in Big Data: Privacy and Data Mining [J] Access IEEE, 2014, 2:1-28. DOI:10.1109/ACCESS.2014.2362522

作者简介

华新海，中兴通讯股份有限公司多媒体视讯产品总经理；主要研究方向为云计算、基于 IP 的视频产品技术与解决方案、视频业务安全解决方案、内容分发网络技术与产品解决方案等。

贺镇海，中兴通讯股份有限公司多媒体视讯产品线产品规划经理；主要研究方向为网络安全、视频业务智能检测等。

刘志军，中兴通讯股份有限公司多媒体视讯产品线产品经理；主要研究方向为多媒体视频业务的智能安全检测、防范技术与产品解决方案等。