The Potential and Security of 5G for Broadcasting

Tom Macey - Supervised by: Raja Akram & Konstantinos Markantonakis
Information Security Group, Smart Card and IoT Security Centre

The Smart Card and Internet of Things Security Centre

Objectives

To research and identify the risks of implementing 5G-based content delivery in broadcasting at all stages.

Specifically:

- Identify what areas of a broadcast network are most vulnerable to attacks
- Analyse the consequences of different types of attacks
- Present solutions to mitigate or reduce the risk of attacks.
- Explore the potential for broadcasting over an IP-based network with virtualised network functions.

Introduction

5G is the latest generation of mobile network communication systems.

The IoT, along with other new technologies such as cloud computing, network function virtualisation and software-defined networking will be implemented into 5G, meaning more devices will be able to access the internet through 5G networks.

In line with the rest of the world, earlier this year, 5G was launched in major cities across the UK. Network carriers are set to introduce the infrastructure to the rest of the country over the next few years.

Not only is 5G an improvement upon the current 4G network, but it also introduces many new possibilities for a myriad of use cases.

One such use case is broadcasting. The BBC has run trials of both TV and radio broadcasting over the 5G network in preparation for a new industry paradigm which delivers content over the internet instead of digital terrestrial, cable or satellite communications. However, in both broadcasting and 5G, there are security vulnerabilities that must be considered in order to prevent misuse of content or other sensitive data.

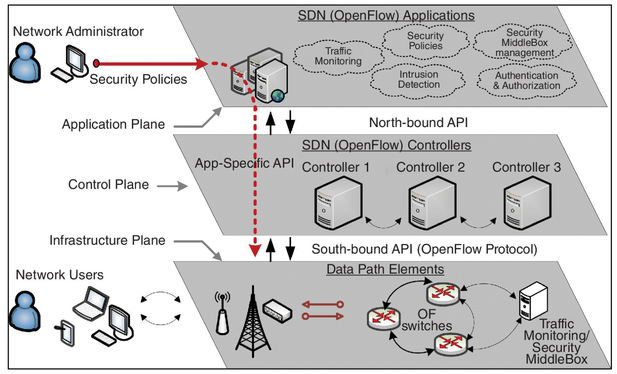

Figure 1: Diagram of a Software-Defined Network (OpenFlow) [1]

Security Vulnerabilities

In any industry, a cyber attack can come in several forms at varying degrees of scale. Most are conducted with the aim of stealing data for exploitation.

The biggest threats facing both 5G and broadcasting are:

- Data theft, personal information about customers or employees could be stolen and sold to third-parties.
- Denial-of-service attacks, can shut down a website. Could halt broadcasts over a 5G network.
- Content piracy, leaking premium content before intended release, redistributing content for free or for profit
- Signal hijacking, organised crime groups or other malicious organisations hacking broadcaster's network to broadcast their own content

In April 2018, a survey was conducted by cybersecurity firm Akamai in which 200 media organisations answered questions about what concerns they have with their company related to cybersecurity. Only 1% said they were 'confident' in their security solutions.

Cybersecurity issue	Companies concerned
Slow site performance and security measure downtime	26%
Protecting premium video content	23%
Security of enterprise applications	20%
Managing bot traffic	15%
Mitigating DDoS attacks	17%

Figure 2: Akamai survey results for media company concerns [2]

Akamai also asked the companies they surveyed about what types of attacks they have encountered.

Type of attack	Companies affected
SQL injection	23%
DNS attacks	21%
Pirated content	20%
DDoS attacks	17%

Figure 3: Akamai survey results for media company attacks [2]

Other attacks reported include hacked accounts, defaced websites and cross-site-scripting.

DDoS Attack Mitigation Tactic	Companies using tactic
Network firewalls in data centres	31%
Dedicated mitigation 'scrubbers'	26%
Intrusion prevention systems in data centres	17%
Mitigation through ISPs	11%
Cloud-based content delivery networks	14%

Figure 4: Akamai survey results for DDoS attack mitigations [2]

Lab Setup

To help understand how 5G can be used as a means of broadcasting, I decided to simulate a software-defined network in the lab. 5G is built around SDNs which minimize the need for function-specific hardware.

Originally, I was going to try creating several virtual machines running Ubuntu Server 18.04 LTS, each connected to an internal network with programs dedicated to a specific function. But this turned out to be too complex to complete within the time frame. So instead, I have created a media centre using OpenStack to broadcast a video over the cloud.

The software I have used for this are listed below.

- Ubuntu Desktop 18.04 LTS (Host)
- OpenStack (DevStack)
- Ubuntu Server 18.04 LTS (OS Instance)
- Plex Media Server

Running the Software

I installed the DevStack version of OpenStack on my host Ubuntu system by cloning the master branch from the official Git repository to the host's local filesystem. Creating a configuration file enabled me to tie the host's IP address to the cloud running on the machine.

Once installation was complete, I added rules to the default security group to allow SSH and ICMP access within Royal Holloway's network. An SSH key pair was created and saved to the host's local hard disk.

Next Steps

Currently, I am in the process of setting up the instance of Ubuntu Server on the OpenStack cloud. I will be using systematic problem-solving so that the instance will be fully operational. After this is completed and Plex Media Server is installed and running on the instance, I plan to introduce a type of cyber attack to the cloud server to see how the broadcast is affected.

References

[1] Liyanage, M., Ahmad, I., Abro, A., Gurtov, A. and Ylianttila, M. (2018). A Comprehensive Guide to 5G security. Wiley.
[2] DeNisco Rayome, A. (2018). Only 1% of media companies are 'very confident' in their cybersecurity. [online] TechRepublic.
Available at: https://www.techrepublic.com/article/only-1-of-media-companies-are-very-confident-in-their-cybersecurity/ [Accessed 2 Jul. 2019].

Acknowledgements

Raja Akram @ RHUL
Konstantinos Markantonakis @ RHUL

Contact Information

- Web: https://scc.rhul.ac.uk
- Email: Tom.Macey.2018@rhul.ac.uk