Multimedia IP networks as critical infrastructure

Gergő Juhász[1], Róbert Sándor Dr. Kovács[2]

[1]Obuda University, Doctoral School of Security Science, József körút 6., Budapest, 1088, HUN, juhasz.gergo@kvk.uni-obuda.hu

[2] Obuda University, Kandó Kálmán Faculty of Electrical Engineering, Institute of Electronics and Communication Systems, Department of Telecommunications and Infocommunications, Bécsi út 96/B, Budapest, 1034, HUN, kovacs.robert@kvk.uni-obuda.hu

Abstract: Multimedia IP-based communications, especially IPTV, streaming, and video sharing services, play a key role in today's information-based society. These systems are not only used to provide entertainment content, but can also be essential tools for everyday information, news services, and even emergency communications. As an increasing part of the citizens access information through these channels, their function, reliability, and security have become critical. Multimedia IP networks can therefore now be classified as critical infrastructure, not only from a technological but also from a social perspective. The security risks of this technology are increased by the fact that these systems are based on the same protocols as traditional data transmission IP networks, and therefore have similar vulnerabilities and attack surfaces. In the case of a successful attack, the attacker may be able to manipulate content and broadcast illegal or disinformation programs, which could lead to mass deception, panic, or ideological influence. A similarly serious problem can arise if the service becomes unavailable due to a cyberattack, as in a critical situation—such as a natural disaster, war, or terrorist attack—the population will not be able to access reliable information in a time-sensitive way. In this case, it is not just a simple technical problem, but also a security risk at the public level, as the lack of reliable information flow can lead to public insecurity and social instability. In such cases, the goal is not only economic benefits, but also influencing society. The consequences of such attacks can be particularly serious in countries where there is armed conflict or political instability, as attackers can directly influence the ideology and decisions of the public by manipulating multimedia channels. The security assessment of multimedia IP networks is therefore no longer just an IT issue, but is also of key importance from a national security and social security perspective. The aim of my research is to show why these networks can be considered critical infrastructure and what dangers their vulnerability represents.

Keywords: cybersecurity; critical infrastructure; multimedia; IPTV; stream

1 Introduction and motivation for the choice of topic

The explosive growth of multimedia IP networks over the past decade has fundamentally transformed the market for media content production and distribution, and with it consumer habits. Billions of people around the world access news, movies, live broadcasts, and educational content through streaming platforms that operate entirely on IP-based networks. This new model of content consumption is particularly sensitive to network parameters, infrastructure availability and stability, and service providers' attitudes towards emerging security issues.

Research has so far focused primarily on these security issues in the IT, business, and industrial segments. Numerous engineers and IT specialists work in this field on a daily basis, tasked with preventing cyberattacks, recovering from any incidents that may occur, and educating employees about security awareness. In contrast, however, we can see that both in research and in real life, the security testing and research of IP networks used specifically for the transmission and distribution of multimedia content is significantly underrepresented. This may be critical in the light of the fact that, due to the widespread use of these networks, they form the basis of mass communication today, and therefore control over media content and its transmission is a key issue in modern society.

The choice of topic for my PhD research was motivated by the realization that very limited scientific research has been conducted in the field of security engineering for multimedia IP networks. While a significant amount of literature deals with general security issues in classic computer networks, the examination of IP-based systems specifically designed for the transmission of multimedia content has received much less attention in academic circles to date. A significant part of the literature has analyzed the technical and service developments, operation, and structure of streaming technologies primarily from the perspective of network parameters and quality improvements. The reason for this is that one of the most important criteria for services was to reduce network latency, improve compression efficiency, and maintain network stability. These publications already suggested that IP-based content delivery is a much more complex system than the previous broadcast-based broadcasting, but security considerations were only mentioned in passing. [1]

At the same time, the spread of multimedia IP -based services in society has increased significantly, and with it, their potential security risks. Streaming platforms are now not only entertainment industry participants, but also key factors in social communication, information flow, and citizen information. At the same time, attacks and manipulations against platforms have not only technical but also social significance, especially when the modification, replacement, or blocking of content can affect the public's access to information. This has already been emphasized in recent security science literature, which states that attacks

against modern communication infrastructures have become part of cyber warfare, especially through the manipulation of digital media channels. [2]

The relevance of this research is further reinforced by the fact that multimedia IP networks – although often considered commercial services – actually play a critical role in providing information to the public. These systems transmit content that influences the functioning of society, decision-making processes, and even security policy. If a streaming platform has vulnerabilities or can be manipulated, the consequences of a targeted attack go beyond the scope of a simple technological problem. From a security science perspective, therefore, the examination of multimedia IP systems is necessary and justified.

My choice of the topic is also motivated by my professional background. As an electrical engineer and an employee of the Department of Telecommunications and Infocommunications, I have been working with IP networks, multimedia systems, and telecommunications technologies for several years. In my teaching position, I teach courses on basic networking and multimedia technology every year, during which my own experience has highlighted that multimedia content distribution is a sensitive part of the information and communication era. This led to the realization that this area is particularly important for security science and warrants further research.

2 The development of multimedia communication and its technological challenges

A review of the history of multimedia communication highlights the need to follow developments in order to understand how current IP-based systems work. Traditional broadcasting systems implemented a one-way communication model, in which content flowed from the broadcaster to consumers without interactivity or feedback. These systems ensured stable and predictable operation for many decades, but the digital transition brought technological innovations that enabled new forms of content management and access.

The first steps towards digitization, such as DVB systems, resulted in higher quality and better spectrum efficiency, but broadcasting remained fundamentally centralized (broadcast-like). The change became significant when IP-based networks became capable of transmitting large amounts of multimedia content. In the development of streaming technologies, the literature emphasizes that adaptive bitrate, efficient compression techniques, and real-time error correction enable modern video services that are now capable of two-way, interactive communication. However, these developments could only become widely used by improving network reliability through the introduction of QoS (Quality of Services). [3]

One of the most important pillars of modern multimedia systems is the appearance of content delivery networks, or CDNs. CDNs enable content to be physically closer to users, which reduces latency, increases service efficiency, and balances sudden increases in load. The operating principle and architecture of CDNs are therefore essential for ensuring the stability of streaming services. The development and operation of CDNs themselves carry security risks, as the fragmentation of content increases the attack surface. [4]

The arrival of streaming and IPTV systems has brought with it a complex, multi-layered infrastructure in which content is produced, encoded, distributed, and consumed using IP-based technology, involving a significant amount of real-time data processing. This complexity also means that security testing poses a particularly big challenge.

3 The role of QoS and the balance between security solutions

One of the most important technical requirements for streaming services is ensuring proper QoS. Delay, packet loss, jitter (delay fluctuation), and bandwidth fundamentally determine the quality at which users can consume multimedia content. There are several methods for ensuring QoS, including network traffic segmentation, priority management, and adaptive resource allocation. Some research indicates that artificial intelligence-based predictive modeling can optimize QoS by enabling the network to respond to traffic fluctuations in real time. [5]

However, the question of how to achieve a continuous balance between QoS and security remains an open issue. The encryption and authentication mechanisms used in streaming systems often require more computing capacity and longer packet processing times, which can increase latency. Packet inspection procedures and various content authentication methods can also slow down content delivery, forcing service providers to constantly seek compromises between user experience and network security. This is particularly important where content arrives in real time, such as in the case of live broadcasts and interactive programs. [6]

4 Multimedia IP networks as critical infrastructure

The importance of multimedia services in the flow of information has become significant enough to raise the following important question: can these systems be considered critical infrastructure? The literature on critical infrastructure

protection emphasizes that this category includes infrastructure whose operation fundamentally affects social stability, economic processes, and the functioning of the state. Although at first sight multimedia systems may appear to be commercial services, in reality a significant part of the population accesses public, political, and social information through them. [7]

An attack on a streaming system, content replacement, or cover-up can therefore have a destabilizing and destructive effect on society. In a crisis situation, it can be particularly dangerous if the public is misinformed, manipulated, or not informed at all. Modern security science literature provides several examples of how the manipulation of information systems has become a tool of hybrid warfare, in which the goal is often not direct physical damage, but rather the destabilisation of trust and the intensification of social tensions. Targeted disinformation content disseminated on multimedia platforms can influence political decisions, election results, and national security measures. Disrupting critical infrastructure or manipulating its content can therefore have military strategic significance, especially in conflict situations where providing the population with rapid and reliable information is vital. [8]

The economic vulnerability of critical infrastructure is also a significant factor. Streaming platforms are considered to be an industry factor of major economic importance, in which the production, distribution, and sale of content generate huge profits. This can be a serious motivation for economic actors to manipulate content, either by making competing platforms unviable or by causing revenue losses. The literature emphasizes that attacks against multimedia systems are often aimed at causing economic damage and gaining profit, which also influences rivalry between market players. Pirate streaming, content theft, and the unauthorized sharing of paid content cause huge losses worldwide, which becomes a financial motivation for attackers. [9]

Social, political, and economic considerations all argue that multimedia IP systems can indeed be considered critical infrastructure, and that their protection is part of the role of security science. Proving this will be part of my PhD research.

5 Security challenges in multimedia systems

Multimedia IP systems consist of several layers built on top of each other, each with its own specific security risks. Threats in the network layer often include route hijacking, denial-of-service attacks, and other network manipulations aimed at redirecting or disrupting traffic. In CDN systems, the main threats are server-side attacks and distribution network paralysis, which can cause content damage and prevent transmission. Vulnerabilities in streaming encryption methods, such

as unencrypted or poorly protected communication channels, facilitate unauthorized decryption or modification of content. [10]

End devices such as smart TVs and set-top boxes are particularly vulnerable, as these consumer devices often lack the necessary security updates and protections. The literature repeatedly points this out, indicating that device vulnerabilities on the user side often compromise the home network and related services. These types of attacks are particularly problematic because they are difficult for service providers to detect and often only come to their attention after the fact. [11]

The server-side infrastructure of streaming providers can also be a target for attacks. Denial-of-service attacks, data theft, and server-side manipulation threaten the quality and reliability of the service. Techniques designed to circumvent authorization systems also pose a serious threat, as they aim to distribute paid content illegally, causing significant financial damage to service providers. According to the literature, the attack surface of streaming systems is much larger than one might first assume, and due to real-time content delivery, recovery time is also much shorter than for traditional systems. [12]

6 The role of the human factor in multimedia system security

The human factor continues to play a key role in the security of multimedia IP systems. A significant proportion of users do not have the digital skills required to use online services securely. Using weak passwords, using the same login credentials across multiple platforms, and installing unknown applications or plug-ins are all mistakes that increase risk. Lack of digital awareness can be particularly dangerous in cases where users enter sensitive data on streaming platforms.

An important element of my PhD research is therefore a questionnaire-based human study, which aims to explore the digital security habits of different age groups, their perception of risks associated with streaming platforms, and their attitudes towards data protection. Examining the human factor helps us understand how user behavior increases the success of attacks and what measures are needed to raise awareness.

7 The role of technical testing in protecting multimedia IP systems

One of the major parts of my research is the technical analysis of multimedia IP systems. During my research, I plan to build a test network that can model real streaming traffic and services. The test system will include IPTV and OTT (Over the Top) elements, a CDN model, real-time encoders, and a variety of end devices. During the technical tests, I will analyze targeted attack attempts to determine which layers are most vulnerable.

Comparing encryption and authentication systems will also be an important part of my work. The effectiveness of different DRM (Digital Rights Management) systems, the security of key management processes, and the reliability of content authentication methods are all issues that determine the vulnerability of streaming systems. When examining end devices, I will analyze attack techniques that exploit software or hardware vulnerabilities in the devices. These devices are often underprotected and, in many cases, cause problems on the user side.

The vulnerability assessment of CDN structures is particularly important, as these content distribution points are the most critical elements of streaming systems. Load attacks and server-side intrusions are both forms of attack that can cause significant damage to CDN layers and seriously compromise the authenticity of content. With the help of these tests, I aim to develop a methodology that places CDN security testing within a unified framework.

8 Description of the four-year research plan

The four-year PhD research project aims to develop a comprehensive security methodology that examines multimedia IP systems from both a human and technical perspective. The first year of the research will involve a review of the literature and a questionnaire survey to identify risks arising from user behavior and digital security vulnerabilities. During the second year, I will build a test network environment that will enable the simulation and analysis of real streaming traffic.

The main focus of the third year is to conduct technical vulnerability tests. During this period, encryption and authentication systems will be compared, terminal equipment vulnerability will be tested, and CDN security tests will be conducted. The fourth year will be devoted to developing the methodological framework for the research, resulting in a complex security model capable of covering all critical elements of multimedia IP systems.

Conclusion

The examination of multimedia IP networks is of high importance from the perspective of modern security science, as these systems represent one of the most decisive sources of information flow in society. The vulnerability of streaming services is not only a technical issue, but can also have economic, social, and political consequences. The aim of my doctoral research is to develop a comprehensive model that examines the security challenges of multimedia IP systems from multiple perspectives and formulates protection recommendations that contribute to increasing the system's resilience.

References

[1] Qin Xin, Mamoun Alazab, Rubén González Crespo, Carlos Enrique Montenegro-Marin, AI-based quality of service optimization for multimedia transmission on Internet of Vehicles (IoV) systems, Sustainable Energy Technologies and Assessments, Volume 52, Part A, 2022, 102055, ISSN 2213-1388, https://doi.org/10.1016/j.seta.2022.102055.

[2] Michael Oche, Rafidah Md Noor, Johnson Ihyeh Aghinya, Network centric QoS performance evaluation of IPTV transmission quality over VANETs, Computer Communications, Volume 61, 2015, Pages 34-47, ISSN 0140-3664, https://doi.org/10.1016/j.comcom.2014.12.001.

[3] Paul Ganley, Copyright and IPTV, Computer Law & Security Report, Volume 23, Issue 3, 2007, Pages 248-261, ISSN 0267-3649, https://doi.org/10.1016/j.clsr.2007.01.005.

[4] Chaeyun Jang, Seongcheol Kim, Kids content as IPTV operator's new differentiator: The Korean case, Telecommunications Policy, Volume 48, Issue 6, 2024, 102765, ISSN 0308-5961, https://doi.org/10.1016/j.telpol.2024.102765.

[5] Kristina Irion, Natali Helberger, Smart TV and the online media sector: User privacy in view of changing market realities, Telecommunications Policy, Volume 41, Issue 3, 2017, Pages 170-184, ISSN 0308-5961, https://doi.org/10.1016/j.telpol.2016.12.013.

[6] Naoya Sekiguchi, Hidema Tanaka, BGP hijack attack policy against AS topology map, Internet of Things, Volume 25, 2024, 101059, ISSN 2542-6605, https://doi.org/10.1016/j.iot.2024.101059.

[7] Steven Branigan, Securing the Critical IP Infrastructure, Information Security Technical Report, Volume 7, Issue 2, 2002, Pages 57-64, ISSN 1363-4127, https://doi.org/10.1016/S1363-4127(02)02007-1.

[8] Günter Knieps, Internet of Things, critical infrastructures, and the governance of cybersecurity in 5G network slicing, Telecommunications Policy, Volume 48, Issue 10, 2024, 102867, ISSN 0308-5961, https://doi.org/10.1016/j.telpol.2024.102867.

[9] Roberto Caviglia, Daniyar Aliaskharov, Alessio Aceti, Mila Dalla Preda, Paola Girdinio, Giovanni Battista Gaggero, A Security Operation and Event Management (SOEM) Platform for Critical Infrastructures Protection, Computers, Materials and Continua, Volume 85, Issue 3, 2025, Pages 5327-5340, ISSN 1546-2218, https://doi.org/10.32604/cmc.2025.068509.

[10] Jiwhan Kim, Changi Nam, Min Ho Ryu, IPTV vs. emerging video services: Dilemma of telcos to upgrade the broadband, Telecommunications Policy, Volume 44, Issue 4, 2020, 101889, ISSN 0308-5961, https://doi.org/10.1016/j.telpol.2019.101889.

[11] NianMin Yao, JinZhong Chen, Guaranteed Quality of Service in Multimedia System, Procedia Engineering, Volume 24, 2011, Pages 287-291, ISSN 1877-7058, https://doi.org/10.1016/j.proeng.2011.11.2643.

[12] Li Kuang, Zhifang Liao, Wentao Feng, Haoneng He, Bei Zhang, Multimedia services quality prediction based on the association mining between context and QoS properties, Signal Processing, Volume 120, 2016, Pages 767-776, ISSN 0165-1684, https://doi.org/10.1016/j.sigpro.2015.01.013.