Network Security for Broadcast Media Streaming

Keyur Parikh and Junius Kim
GatesAir
Mason Ohio

Abstract – *IP Networks have become ubiquitous as broadcasters are not only using them for managing their equipment, but also increasingly using them for transporting broadcast media for contribution and distribution. IP Networks provide clear benefits in both cost and flexibility. However, the TCP/IP protocol suite also opens up security risks that can de-stabilize the system's operations and impact real-time media services. In this paper, we will describe methods used to create security risks on a streaming platform such as: Denial-of-Service attacks, compromise of the management plane, eavesdropping and hijacking of media streams. We will then describe various counter measures that can be implemented to mitigate these risks in the form of operational practices and integrated security features within the streaming platform.*

THE MIGRATION TO AN ALL IP NETWORK

Over the past one and a half decades, we have seen the traditional voice services go through a transformational process from using circuit switching to Voice over IP (VoIP). The same is occurring in the broadcast industry. Over time, an increasing number of vendors started supporting the TCP/IP Interface with the embedded web server and a SNMP agent for equipment management. This allowed broadcasters to use standard web browsers for equipment control and have their operational network connected to their enterprise network. While the management plane transitioned to using IP, the media plane remained on circuit switched paths. Over the last few years, the transition to using wide area IP networks for contribution and distribution of broadcast media has accelerated. As a result, the equipment vendors have been incorporating capabilities to natively stream audio and video over IP using industry standard protocols such as SIP and RTP. In some cases, the wide area IP networks are private and controlled by the broadcasters. However, in most cases, they are provided by an independent Internet Service Provider (ISP). While this migration provides benefits in both cost and flexibility, it also exposes the broadcast equipment to the same security threats that are faced by other networked devices, such as those used by VoIP applications. The use of firewalls at the network perimeter to filter incoming unsolicited traffic is a common counter measure. This filtering does provide an effective outer layer protection for the devices. However, in many instances, special exceptions have to be setup within the firewall to allow legitimate traffic of the broadcast equipment to flow. These exceptions in turn can be exploited to launch an attack on a target inside the network. In the past, these attacks required detailed knowledge of networking protocols. Today, with all of the tools available, someone with an average skill set can become a successful attacker.

MOTIVATION FOR THE ATTACKER

There are two primary motivations for network attacks: stealing information and disruption of services. Stealing of information can range from online thieves using victim's personal information to steal cold hard cash – such as someone fraudulently using victim's bank account or credit card information. This is most likely to occur in consumer spaces, where the attacker can use malware (malicious piece of code) to gather critical information from the victim's computer or use technique such as Phishing which utilizes fraudulent websites to trick users to submit their credentials. A more organized form of stealing is in the form of corporate or international espionage. This is where highly skilled computer programmers launch an attack on internal servers using sophisticated techniques to steal valuable information. Although it is important to understand the above type of threats, they are generally not a concern within the broadcasting environment.

An attacker looking to disrupt the network or services of an equipment may be motivated by several factors such as: a disgruntled employee within the organization or someone from outside the network motivated by competitive reasons or simply the thrill. For broadcasters, these types of attacks are a real threat, especially as their use of ISP networks increases.

SECURITY PARADIGM FOR BROADCAST EQUIPMENT

Before we get in to the specific types of attacks, let us first understand what it is that we are securing. Security in general is about protecting your assets. This has a different meaning depending on the type of services the asset is providing. As with any other networked device, broadcast equipment relies on the following security foundations:

Authentication – Provides identification of the client that is connecting to the system services. For example, Human-Machine interaction involves authentication of the user to connect to the management applications (i.e. web server, SNMP agent etc.), Machine-Machine interaction involves authentication of peer equipment for exchanging media traffic using protocols such as SIP and RTP.

Authorization – Primarily for Human-Machine interaction. It provides restrictions on the user’s view of the system or the ability to make changes based on operational roles. For instance, making system changes may be restricted to the lead engineer, while the operator personnel may be restricted to what is needed for trouble shooting.
Auditing – Process of providing an audit trail of configuration changes made to the system by an Authenticated and an Authorized end user.
Confidentiality – This is also referred to as privacy. This process ensures that eavesdropping of management or media traffic is not possible. This is accomplished by using encryption of management and media sessions.
Availability – From a security perspective, this is the measure of the broadcast equipment ability to thwart off Denial-of-Service (DoS) attacks and remain operationally available.

Types of Attacks

In the consumer space, it is a well known fact that Microsoft Windows based laptops and desktops bear the brunt of the attacks. One of the main reasons for this is the sheer volume of devices that run the Windows operating system. Also, in most use cases, the applications are client driven which increases the potential of users clicking on malicious links on web browsers or Emails.
Broadcast equipment, on the other hand, generally runs on embedded or hardened operating systems with application services or protocols that are limited to system management and media streaming – see Figure 1.

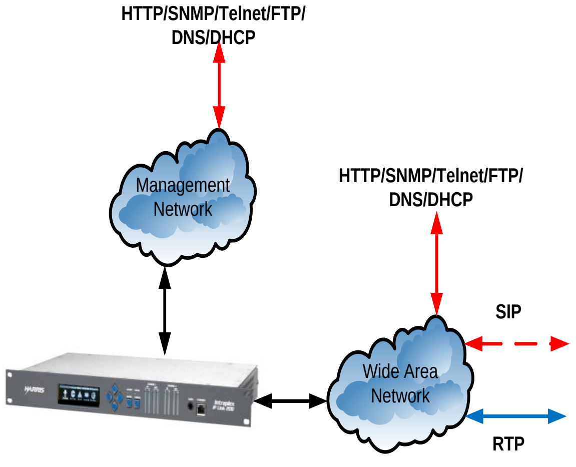

Figure 1 Network Architecture for Audio over IP

Furthermore, these applications are primarily used in a server mode and therefore threats associated with user initiated actions, such as clicking on malicious links, are absent. It is also more difficult to get malicious code to execute in these devices because of the way the programs are compiled and linked in the embedded operating system environment. However, these devices are vulnerable to other types of threats such as:

- Unauthorized system access via management applications such as: web server, FTP, Telnet, and SNMP services etc.
- DoS attacks to disrupt the operation of the system
- Tampering and hijacking of media traffic

Let’s analyze each threat in more detail.

Unauthorized Access to the System

TCP/IP protocols such as embedded web (HTTP) server, FTP server, Telnet server or SNMP agent allow users to manage the equipment. Someone who gains successful access to the management plane with the proper credentials to modify system configurations can cause unlimited damage. The first step in initiating such an attack is to identify the type of services or protocol server that are running on a system. This can be accomplished in several ways: an inside attacker might already have this information through “Social Engineering” means. An outside attacker might perform a port scan on a system to determine which services are active and determine the underlying operating system which can provide specific vulnerabilities to attack. For example HTTP listens for client connections on TCP Port 80, FTP server listens for connections on TCP port 21, etc. Once the services are known, an attacker can either use the brute force method to crack usernames and passwords or sniff unencrypted traffic to steal the credentials. With the prevalent use of embedded web servers on these devices, threats from hacker methods that are commonly used to gain login credentials on web servers, such as Cross-Site-Scripting (XSS), or Dictionary attacks are present even if using Secure Socket Layer (SSL) protocol to secure the web connection. In the XSS attack, the hacker injects malicious client side script using user defined fields on a web form, the script on this form is then executed by the victim’s web browser when they log on to the system’s web page. In most instances, these types of attacks are meant to steal the victims’ session cookies to gain access to the system. The Dictionary attack, which is the most common threat in this environment is meant to guess the password of the victim using an automated tool which attempts to figure out the password by trying different combinations. Threats such as SQL Injection attacks or remote code executions are less common in these devices since, in most instances, the systems do not utilize a SQL database or use server side scripting such as PHP for back-end processing. In most cases, the back-end processing is done using compiled languages such as C or C++, which makes this process very difficult.

Denial of Service (DoS) Attack

The single most threat to a network equipment from an outside attacker is (DoS) attack via the service ports that are open for outside communication. The purpose of the DoS attack is to consume the system’s resources so that it is not able to process or respond to legitimate traffic, thus crippling the capabilities of the system to provide the intended services. Some examples of such attacks are:

Ping Flood – The TCP/IP Ping program uses ICMP protocol. It is a basic utility program used to detect reach ability of a device. It works by sending an ICMP Echo Request packet to the target system, which, in turn, responds with an ICMP Echo Reply packet. The attacker using this utility program can flood the target system with ICMP Echo Request packets which, then, can get overwhelmed with processing them and cause resource exhaustion.

TCP SYN Flood – The application services such as HTTP, FTP, Telnet and Secure Shell (SSH) use TCP as the transport protocol. A bi-directional TCP connection setup involves a 3 way handshake between the client and the server. The exchange starts off by a client issuing a connection request to the server on its "well known" port. The server responds with an acknowledgement for the forward connection and also issues a connection request back to the client for the reverse connection. The final message of the handshake is a client acknowledgement to complete the bi-directional connection. This is illustrated in the Figure 2.

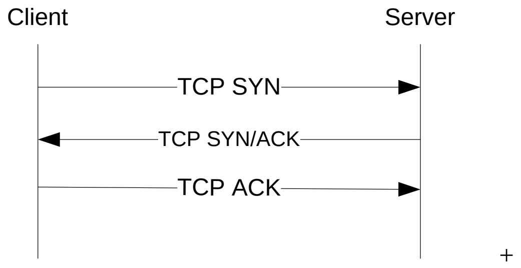

Figure 2 TCP Handshake

An attacker using the 'TCP SYN Flood" tactic can inundate the server with TCP connection requests without actually going through the process of completing the connection. This in turn can exhaust the system's processing resources, causing it to be unreachable to legitimate users.

IP Fragmentation Attacks – IP packets are fragmented when they exceed the Maximum Transfer Unit (MTU) of the interface. The fragmentation process breaks the original IP packets in to multiple smaller packets so that each packet fits within the MTU of the interface. The destination system buffers up individual IP fragments until a packet is completely received. The fragments are then re-assembled at the destination node to re-create the original IP packet before sending it to the TCP or UDP layer. An attacker can exploit this process by using some known vulnerability in the operating system's TCP/IP stack by sending invalid fragmented packets, which in turn can cause the exhaustion of system's buffer resources or unpredictable behavior in TCP/IP stack. In some instances, these exploits include: sending excessive number of IP fragments or sending oversized payloads or sending overlapping IP fragments.

ICMP Error Generation **–** The ICMP Error messages are automatically generated by the receiving TCP/IP stack towards the sender when it encounters processing errors. Some of these error messages are also used by network utility program such as: Path MTU Discovery and Trace Route. A system may experience resource exhaustion if it is made to send these error messages at a very high rate. This is possibly due to an attacker intentionally sending packets that cause the receiver to enter the error generation state. Another use of the ICMP Error messages by an attacker is to "finger print" or determine the operating system of the equipment. Once the operating system is known, the attacker might use its known vulnerabilities to launch specific attacks.

Tampering and Eavesdropping of Media

TCP/IP communication between two networked devices can be eavesdropped upon or intercepted by what is commonly known as a Man-In-Middle attack. An unencrypted communication using open standard protocols can be eavesdropped upon by sniffing the traffic at an intermediate Ethernet switch or a router. In a more severe case, the attacker can hijack a session by acting as a proxy between the communicating parties, thereby, not only eavesdropping on the traffic but potentially modifying it – see Figure 3.

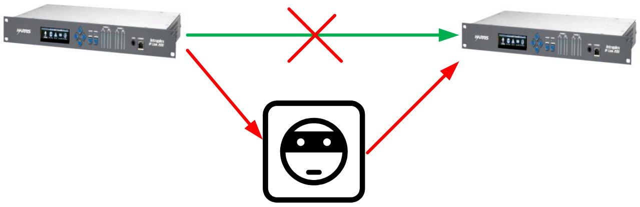

Figure 3 Man-In-Middle Attacker

Within the broadcast industry, there is a push to move towards open standards protocols for interoperability between equipment of different vendors. While the use of open standards is good for interoperability, it also means that details of the protocols used for media transport are readily available to everyone. For instance, European Broadcast Union (EBU) has standardized using SIP with RTP and RTCP for Audio over IP transport. The SIP protocol carries the signaling information, while RTP carries the actual media. This specification calls for industry standard media algorithms to be used with RTP payload formats that are specified in IETF RFCs. The SIP and RTP specifications were originally developed for the VoIP industry but have since been adapted to transport any type of media. The SIP, along with its companion, SDP, specification is used for signaling the encoding and payload formats of the media carried within in the RTP packets. For some common media formats, the IETF has defined the standardized format for RTP. As a result, the SIP and SDP signaling may not be necessary to determine the media carried within the RTP packets. Some examples of the standard RTP media payloads are G722 and L16.

An attacker interested in eavesdropping on the media can intercept the SIP signaling packets to determine the type of media and its format carried with the corresponding RTP packets. Effort to counter this risk may depend on the sensitive nature of the broadcast signal. For most commercial broadcasts, this may not be an issue. However, in some cases, media content would need to be protected in transit.

On a more serious case of a Man-In-Middle attack, a person can hijack a RTP stream and start sending their own media to the receiver for broadcast. This can be done on an active stream, where the attacker has learned about the RTP session in progress. It can then intercept the legitimate stream from the sender and send its own stream to the receiver. In another scenario when proper authentication precautions are not taken at the receiver, attackers may simply use SIP to setup a RTP stream with the receiver at the broadcast site and start sending their own media.

What About IPv6?

Where network layer security is concerned, IPv6 is not necessarily more secure than IPv4. The IPv6 does specify the use of IPSEC protocols for security as an optional requirement for a node (RFC 6434). However, one can also run IPSEC currently over the IPv4. As far as application level protocols, such as Telnet, SIP or HTTP are concerned, the threats discussed above are no more or less vulnerable when running over the IPv6 network.

As far as DoS attacks are concerned, generally for IPv4 networks, the streaming devices are behind a NAT (Network Address Translation) router for address translation. Although, NAT routers are not purpose built for security, the commonly used Symmetric NAT technique does provide the first line of security for devices sitting behind NAT by blocking unsolicited traffic. In contrast, in the IPv6 environment, the devices do not need address translation and therefore do not require to be behind a NAT router. Thus, a separate Firewall is required to protect the inside devices for being directly exposed to a wide area network.

The bottom line with IPv6 is that, as proliferation picks up, education and awareness of the protocol will spread, vulnerabilities will be fleshed out, security devices such as Firewalls and Intrusion Detection Systems (IDS/IDP) will be updated, and in time, it will reach the maturity that IPv4 has reached.

Countermeasures

The responsibility to counteract these threats lie both with the broadcast equipment vendors as well as the operators. The equipment vendors should take a cue from vendors of VoIP equipment and start integrating security measures within the equipment. The operators, on the other hand, should keep themselves educated on the latest threats and employ the best operational practices.

Integrated Security Features

Although in most cases, the streaming devices would be protected by a firewall at the periphery, vulnerabilities to the above threats still exist via the open ports. In this section, we list some security capabilities that can be included within the streaming device to help against those threats:

- Programmable IP Access Control List (ACL) per Network Interface that restricts the access to protocol services (e.g. Web, SNMP, FTP, SIP etc.) as well as communication from only specified IP Addresses. For example in *Figure* 1 *Network Architecture for Audio over IP* disabling all protocol services over the WAN network except for media streaming protocols (e.g. SIP, RTP, RTCP).
- ICMP control to restrict the processing rate of the ICMP packets to no more than what is required for normal utility functions. Typically restricting them to a few packets per second should be sufficient.
- Web access protection
  - SSL for authentication and privacy
  - Strong filtering of user populated fields to mitigate XSS type attacks
  - Strong password requirements with mitigation techniques against Dictionary attacks, for example: blocking suspected IP addresses or including a secondary authentication scheme such as a secret question or use of CAPTCHA (“Completely Automated Public Turning test to tell Computers and Humans Apart”)
  - Create user roles for system management. The role based control of the system operation will enhance traceability.
- Logging system configuration changes for audit purpose.
- Support SSH protocol to provide secure file copy or shell access to the system if needed. The SSH protocol provides user and host authentication as well as data integrity and encryption.
- Support authentication and encryption of SIP signaling using the Transport Layer Security (TLS) protocol. The TLS protocol works in a similar manner as SSL. By using TLS, both peers are authenticated and the integrity and privacy of the messages are maintained.
- Support secure RTP for media transport. Secure RTP provides encryption as well as data integrity and authentication. The secure RTP protocol prevents eavesdropping of a media payload by encrypting it using symmetric keys. To prevent session hijacking, the entire payload is hashed with

a secret key and an authentication tag is appended to the end of the packet, which is verified by the receiver system.

Operational Practices

As the complexity and the size of the broadcast network increases, it is important for the broadcasters to take a holistic approach to Network Security. Besides, having integrated security capabilities within the streaming devices, the following operational practices are recommended:

- Secure the outside perimeter of the operational network using Firewall and Intrusion Detection Systems. These are the first line of defense against traffic coming from outside the LAN.
- Keep the operational network traffic separate from the enterprise network. If they are connected at layer 3, separate them at layer 2 using Virtual LANs with limited access between the two segments.
- Use a centralized server to maintain user accounts and profiles and use protocols such as RADIUS or DIAMETER for user authentication. Centralized authentication and authorization servers are more secure than having these accounts distributed across various equipment.
- Utilize the built in security capabilities of the streaming devices such as: IP address based access and selectively enabling protocol services per interface.
- When using ISP networks, the operators should think of end-to-end security. This can be accomplished either by using external VPN equipment or enabling security protocols such as secure SIP or secure RTP. These are mentioned above on the streaming devices.

Conclusion

The Security of the broadcaster's operational network should be examined with a bottoms-up approach, starting with the security of the physical premises to securing the network from attacks emanating from both inside and outside attackers. As the complexity and reachability of these networks grow, so will their security risks. Over the past one and a half decades, mobile and VoIP operators have also gone through this transition. There is a lot that can be learned from these early adopters for both broadcast operators and vendors of the equipment. Broadcast operators should keep themselves up to date on the best practices to follow. For equipment vendors, it is important to integrate security features within the system to thwart common types of attacks. It should be, by no means, the first line of defense, as this equipment is not purpose built for that purpose. The Firewalls and Intrusion Detection Systems must be the first line of defense at the perimeter of the network with the system's built in features as the last line of defense. As we move towards open standard protocols for media streaming, the risk of media tampering or hijacking becomes a real issue. The VoIP industry had faced similar threats. As a result, the protocols that were used for signaling and media transport for the VoIP industry (i.e. SIP and RTP) were upgraded to include privacy and authentication. These same protocols are now increasingly getting specified to be used for broadcast media transport and to mitigate the threat of Man-in-Middle types of attacks. The equipment vendors should be supporting the security features of these protocols.

Author Information

Keyur Parikh is an Architect and Software Lead with GatesAir in Mason, Ohio. Mr. Parikh has over 23 years of experience in design and development of communication systems for various applications. His current interests include architecture and design of systems to reliably transport media over packet based networks. Mr. Parikh holds a BS in electrical engineering with a Master's in communication theory.

Junius Kim is a Hardware Engineer with GatesAir in Mason, Ohio. Mr. Kim was a key member of the Harris design team responsible for creating the SynchroCast simulcasting system and IP Link, a next generation IP audio codec. His current interests include the architecture and design of robust packet switched based telecommunication systems. Mr. Kim holds a BS and MS in electrical engineering.