catalyst communications technologies

A Catalyst Position Paper

Cybersecurity Protections in Catalyst Dispatch Networks

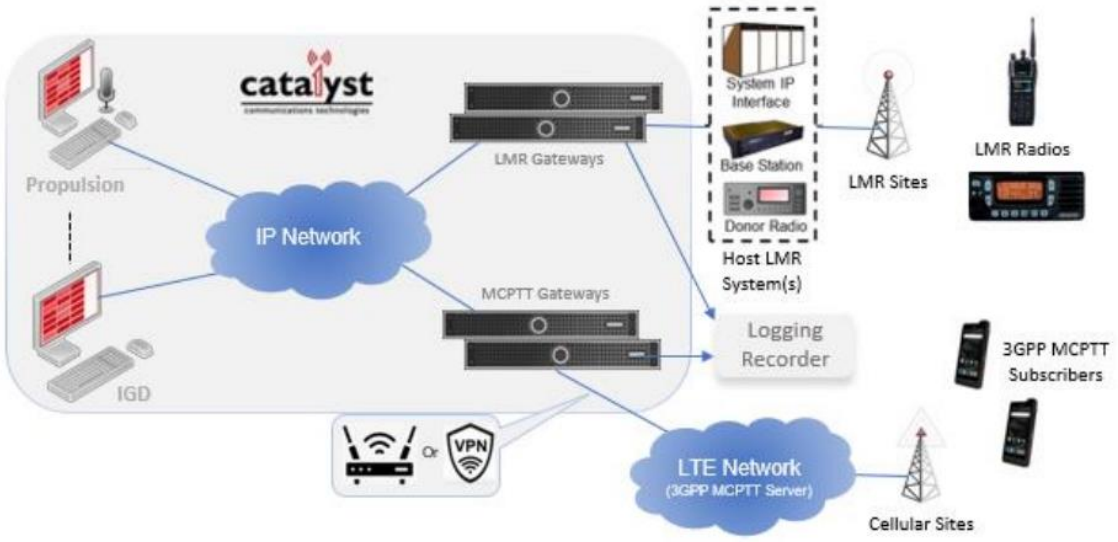
December 2023

Introduction and Purpose

Land Mobile Radio systems are designed to provide instant, reliable and secure push to talk communications to the public safety and first responder communities. The migration of land mobile radio systems from analog to digital has made these networks, devices and data more sophisticated and, because they are digital, more susceptible to cyber threats. While some networks, including those that are architected similar to the Catalyst Communications Technologies architecture, may be considered closed systems and generally not exposed to cyber-attacks, security is still a consideration for these systems. In addition, the inclusion of an LTE Mission Critical Push to Talk application into these LMR networks adds a further level of complexity to cybersecurity planning. This paper identifies areas of risk for cyber-attack on LMR and LTE Networks, with an emphasis on networks designed with Catalyst Communications Technologies' technology and our efforts to protect users on our systems from cyber-attack.

The Catalyst Environment

The Catalyst network architecture consists of computers running Catalyst dispatch software connected to an IP Network that communicate with Gateways. These Gateways are also computers and interface to radio resources, which can be donor radio / base stations, LMR infrastructure, and Gateways connected to LTE networks offering mission critical push to talk services.



In the above diagram the components in the shaded area represent the Catalyst network. Outside the shaded area are radio network components that communicate over radio frequencies to subscribers using portable radios, or in the case of LTE networks, smartphones running push to talk applications. The primary concern of this paper is to describe the risks

associated with components in the Catalyst architecture - the shaded area - while acknowledging that a cyber-attack can target any and all components of a land mobile radio or LTE network.

Catalyst Architecture

A Closed Environment

Referring to the diagram, the Catalyst network is most often architected as a closed network and not connected to the Internet, where most cyber-attacks originate. The security provisions of Catalyst hardware and software - Dispatch and Gateways - will be discussed in detail below. It's true that in many cases the IP Network connecting Dispatch Consoles and Gateways are using the organization's IP Network. Typically, the IT department has implemented robust security for their own internal network, although news reports of cyber-attacks demonstrate that this security is not infallible.

In many cases the network connecting Dispatch Consoles and Gateways, and also including oftentimes radio equipment, are all within a single building using a closed local area network, whose computers never communicate with the outside world.

Protection of Users and Devices

a. Authorization

Authorization is a process by which a computer determines if the client has permission to use a resource or access a file. As described below authorization is combined with authentication that is requesting access.

b. Authentication

For Authentication, the user or computer has to prove its identity to the computer it is communicating with.

Usually, authentication by a computer entails the use of a username and password. Other ways to authenticate can be through cards, retina scans, voice recognition, and fingerprints.

The Catalyst technology uses both Authentication and Authorization to protect Catalyst network components and systems from cyber-attacks. At the Dispatch Console, users are assigned a username and password by an Administrator who has privileges to assign and revoke these log-in credentials. Once authenticated by a valid username and password, the Console automatically sets up communications with Gateways that are authorized to that particular Dispatcher credentials (Dispatchers may be authorized to communicate with all Gateways, or only some Gateways). This authorization communications between Dispatch Console and Gateway is a proprietary protocol that cannot be easily understood by network capture tools, unlike competitors that may use protocols like SIP and RTP that can be more easily deciphered.

c. Managing Users and Identifying cyber-attacks when they occur

Catalyst software – both Dispatch Console and Gateways – includes comprehensive log files that include who and when someone is logged in and can be reviewed to provide insights during and after an event. Many events that are logged can be used to identify the nature of a cyber-attack. Knowing when an attack occurs could further minimize damage to the LMR system, and aid in identifying the appropriate response. Most organizations using LMR or LTE push to talk communications have established plans to deal with a cyber-attack, and the responses that are appropriate for attacks on an organizations IP network are appropriate for any response to an attack on a Catalyst network.

2. Protection of Applications

a. Ability of Catalyst Software to store and activate malicious software

As described above, the Catalyst Network is typically a closed network, running over its own or an organization's IP Network (Local Area Network (LAN) or Wide Area Network (WAN)) but typically not connected to the Internet and not communicating with devices other than those authorized and authenticated for these communications. As such, it's difficult for malicious software to be delivered to and stored on any component of the Catalyst network where it could then be activated through some initiation process. The most practical way for malicious software to enter the Catalyst network would be through RF (radio frequencies) and this data is typically audio communications and meta data associated with that audio – user ID and location, for example. Catalyst software isn't designed to deal with applications or file formats that are not associated with push to talk communications.

3. Protection of Network Infrastructure

a. The Windows Environment and Windows Cybersecurity Protection

b. Typical Network Appliances and Proprietary Cybersecurity Protection

Augmenting the Catalyst cybersecurity initiatives protecting Catalyst components and software from malware intrusion, our systems run on Microsoft Windows platforms that include robust protections provided by Microsoft. These securing protections are comprehensive, from Secure Boot and Trusted Boot help to prevent malware and corrupted components from loading when a device starts, Antivirus protection solutions included in all versions of Windows, and Firewall, VPN, and additional Network Level Security solutions.

In addition to Catalyst Security provisions and Microsoft Security provisions for the operating system our software is designed for, many network components that complete the systems level architecture of Catalyst networks include their own cybersecurity defenses. For example, Cradlepoint, often used for wireless connectivity over IP Networks, recommends best practices for securing the NetCloud Manager Account, securing the local network connecting to a Cradlepoint device, enabling router and internet security, and provide their own Cradlepoint

Secure Threat Management software for deterrence. Cisco Systems likewise provides a catalog of software services on their routers and network interface devices that connect Catalyst components to a network.

4. Summary

The Catalyst components of a LMR LTE solution for critical push to talk communications provide robust deterrence to cyber-attacks, anchored by authentication and authorization services that protect resources from malicious attack. The "closed network" nature of the Catalyst Network environment minimizes the possibility of malicious software entering the network and initiating an activation.

Combined with augmented security from Microsoft and network component vendors, the system level protections against cyber-attacks for Catalyst networks is very robust. While no network can claim complete resistance to cyber-attacks, users of networks including Catalyst components can be confident that a high level of protections against cyber-attacks are present.

Appendix

Department of Defense – Defense Information Systems Agency – Zero Trust Architecture

A zero-trust architecture (ZTA) is an enterprise cybersecurity architecture that is based on zero trust principles and designed to prevent data breaches and limit internal lateral movement. ZT is not a single architecture but a set of guiding principles for workflow, system design and operations that can be used to improve the security posture of any classification or sensitivity level. Many organizations already have elements of a ZTA in their enterprise infrastructure today.

The concept of zero trust has been present in cybersecurity since before the term "zero trust" was coined. The Defense Information Systems Agency (DISA) and the Department of Defense published their work on a more secure enterprise strategy dubbed "black core". Black core involved moving from a perimeter-based security model to one that focused on the security of individual transactions. Zero trust then became the term used to describe various cybersecurity solutions that moved security away from implied trust based on network location (the perimeter) and instead focused on evaluating trust on a per-transaction basis.

As a provider of services to the federal government, Catalyst is committed to supporting our federal organization as they implement Zero Trust, which is a mandate from the Office of the White House, Office of Management and Budget.[1] . Transitioning to ZTA is a journey concerning how an organization evaluates risk in its mission and cannot simply be accomplished with a wholesale replacement of technology. We expect to work closely with our federal, state, local and enterprise partners as they incorporate the principles of Zero Trust over time.

[1] https://www.whitehouse.gov/omb/briefing-room/2022/01/26/office-of-management-and-budget-releases-federal-strategy-to-move-the-u-s-government-towards-a-zero-trust-architecture/