



Secure Multicast Content Delivery with Relevant Security Corp. & Real Privacy Management™ (RPM™) Authentication System

Version 1.0

Table of Contents

- 1: Challenges
- 1: Existing Technologies
- 2: The Solution: Relevant Security and RPM™
- 2: Secure Multicast in Depth: Content Delivery
- 3: Industry Use
- 4: Media Content Providers
- 4: Financial Services
- 4: Military
- 4: RS Multicast: Complete Broadcast Security

Challenges

Today, decisions are information driven and supporting systems use ever increasing amounts of data. Whether protecting secrets or securing intellectual property, dissemination of data quickly, efficiently, reliably, and securely is critically important. Many businesses and industries find themselves in need of secure and reliable multicast content distribution, but struggle to find security products that meet all of these criteria. Traditional technologies can be used, such as VPN, file encryption, or encrypted multicast, however these options do not properly address the particular issues faced in securely delivering content to multiple destinations.

Existing Technologies

Standard VPN technologies scale well for IP uni-cast traffic, however these solutions prove to be inefficient for content delivery because data must be encrypted separately for each connected client. Hardware resource and administrative requirements increase indefinitely with added clients. This approach may be impractical or impossible for broad distribution and/or large quantities of data, particularly when the delivery is regularly occurring, such as is the case with broadcast media, field data, and other continuous information sources.

Encrypted multicast protocol provides the low delay and high efficiency that is lacking in the above options, but includes a weakness shared with the encrypt-then-transfer approach. Information is encrypted with the same key for every client. This presents multiple weaknesses. First, the potential for an attacker to subvert the system by compromising a single client is greater, since the encryption key is shared system-wide. Also, because the encrypted data is being broadcast on multiple vectors, there is a greater surface area for an attack by analyzing the encrypted data.

Existing approaches don't provide a complete solution. Each method outlined exhibits weakness of security, falls short from a performance standpoint, or fails

completely to address the needs of a secure content delivery mechanism. What is needed is a truly new approach to securing broadcast data that is reliable, high performance, and resource efficient.

The Solution: Relevant Security and RPM™

Relevant Security offers the RS security appliances utilizing its patented RPM technology to create the most secure network for the transmission of data, voice, and video on the market.

Combining the flexibility and scalability of a Linux based OS and RPM technology, Relevant Security has developed a secure network appliance which revolutionizes network security. Relevant Security's network appliances not only encrypt all data but also provide strong continuous mutual authentication between the RS appliances at the transmission level allowing users to know for certain their data is secure. The combination of continuous mutual authentication of devices as well as encryption of every transmission provides the strongest security for data in transit. RP is built on top of the very secure AES encryption standard, used by the US Government. AES provides strong data security using 128, 192, or 256 bit encryption keys. The addition of RPM allows a data stream to be encrypted using a new key for each packet or datagram with minimal network and hardware overhead. RPM adds only 5% processing time to each round of encryption. This unique feature of RPM greatly enhances the security of multicast encryption.

RS Multicast from Relevant Security uses RPM to ensure that every multicast datagram is transmitted with a fresh encryption key that is used only once. This means, for example, that a 10GB file when transferred using Secure Multicast will contain over 7.4 million datagram's, each encrypted with a unique key. In comparison, the standard VPN approach with 100 clients would yield only 100 unique keys for the same transmission, while greatly increasing the performance overhead since each client's data stream must be encrypted separately. Applying AES encryption to the multicast broadcast without RPM would yield only one distinct encryption key for the entire transmission.

Rather than changing keys per client to increase data entropy, RS Multicast rotates keys per transaction. This approach combines the performance and efficiency benefits of multicast, and the security of a VPN tunnel to create a robust new approach to secure content delivery. By utilizing Relevant Security's RPM and the flexible multicast transfer features of the OS, Relevant Security is able to offer complete security for content delivery at any scale.

Secure Multicast in Depth: Content Delivery

Secure Multicast can be used as a drop-in replacement for an existing content distribution network. RS Appliances can be installed side by side with existing content servers, eventually replacing the content servers at the edge of the network.

RS Multicast is not a routing protocol, but an IP multicasting application, so security of data is assured from end to end while maintaining compatibility with standard

multicast routing protocols and standards such as IGMP and PIM. Additionally, Relevant Security's comprehensive security and redundancy features are fully integrated. Firewall, VPN, Multi-home and Load Balancer, link encapsulation, and other advanced features allow RS Multicast to integrate seamlessly with the existing network infrastructure.

Content distributors upload a virtually unlimited amount of data to the RS appliance via standard file transfer protocol (FTP). Once uploaded to the appliance, manually or by schedule, files are stored securely until a broadcast is triggered. Broadcasts may be initiated manually or scheduled through the appliance's web administration interface.

Basic configuration parameters include: multicast data address, control channel port, and interface binding. Advanced configuration controls allow the network administrator to determine the precise conditions for the multicast broadcast, including the number of clients required to connect before the broadcast will begin. Fault tolerance is achieved through minimum and maximum wait parameters, so that the broadcast is never delayed due to a failed or temporarily unavailable network node.

Once triggered, the RS Multicast server initiates control channel links with any participating client hosts. The control channel allows each client to acknowledge each received datagram, and submit requests for out of band re-transmissions for any that are lost. The control channel also allows the server to control broadcast bit-rate, avoiding unnecessary retransmissions due to reduced network throughput. A maximum bit-rate may also be set in the server's configuration. The broadcast control channel provides reliability for the multicast transfer without sacrificing the performance benefits.

On the receiving end, each node is left with an exact mirror of the files and directories uploaded to the server. These files can then be offloaded to content and application servers, or stored on the RS appliance until needed. Because RS Multicast uses standard protocols to upload and download data, integration with existing applications and systems is simple and seamless.

Industry Use

RS Multicast is a powerful technology that addresses challenges across industries. Content creation and distribution, financial services, military, and logistics are examples of areas in which RS Multicast can be implemented.

Media Content Providers

Content creators and distributors face increasing threats from piracy, and must be proactive in protecting their intellectual property and that of their customers and partners. Using RS Multicast, content can be disseminated efficiently and in real time to a global audience while protecting the rights of the content creators and owners.

Financial Services

Financial and logistical services rely heavily on real time information exchange over an increasingly large geographic distribution. With the increase in outsourcing and remote workers, organizations must find efficient ways of keeping systems and personnel in sync. By leveraging RS Multicast, these companies can ensure that all resources have access to the latest information. This results in better, faster decisions without putting sensitive data at risk.

Military

Military personnel require real-time intelligence for tactical operations. Using RS Multicast in the field ensures that crucial mission data arrives securely and without delay.

RS Multicast: Complete Broadcast Security

Because Secure Multicast is built on the OS's powerful application platform, interoperability, reliability, and implementation methods and challenges are well understood. RS Multicast can be rolled out over time, and operate side by side with existing equipment. Redundancy can be achieved at both the hardware and software level, maximizing uptime and reducing or eliminating recovery time.

RS Multicast provides complete broadcast security while conserving network resources and ensuring reliability. Relevant Security's RPM is the technology necessary to provide multicast security that combines the security benefits of traditional VPNs with the speed and efficiency of Multicast and the reliability provided by our Linux OS Multicast features. RPM enhances the security of standard encrypted multicast by providing group re-keying at a rate of once per datagram. This level of security through RPM differentiates RS Multicast from all other competitors.

For more information

Secure Multicast Content Delivery: www.rscorp.com/library/whitepapers/smcd

RPM™ details: www.rscorp.com/rpm



Relevant Security Corp.
990 South Broadway, Suite 400
Denver, CO 80209

Toll Free: +1-877-576-9665
Phone: +1-720-836-7350

www.rscorp.com