AT&T Telepresence Solution®

Security Building Blocks and Principles

Telepresence is a videoconferencing solution that differs from conventional video systems because it uses "life-size" ultra high-definition video images (1080p), CD-quality audio, interactive technologies and specially-designed room environments to give users the feeling of actually being in the same room with participants located in their own telepresence rooms. AT&T Telepresence Solution provides end-to-end deployment and management of telepresence using the AT&T global MPLS network. AT&T Telepresence Solution reliability is built around the AT&T highly reliable and secure MPLS network, which provides Class of Service priority delivery of real-time telepresence traffic.

AT&T Telepresence Solution is provided as a comprehensive bundled solution that includes network-based meet-me and business-to-business conferencing capabilities using the AT&T Business Exchange. Depending on the deployment model selected, customers may access, schedule and manage their conferences by using a centralized web portal or using their own corporate scheduling systems (such as Microsoft® Outlook or Lotus Notes®).

The AT&T legacy and expertise lies in the creation and maintenance of reliable, feature-rich services and networks. Building on the established dependability and resiliency of the AT&T network, AT&T Telepresence Solution was also architected to a set of strict security protection methods and procedures. This brief article explains these security building blocks and principles underlying AT&T Telepresence Solution.

Discussed in this article are the important concepts of Separation, Control, Validation, Response and Encryption/Authentication.

Customer Separation

AT&T Telepresence Solution customer traffic is kept separated from other customer traffic using the traffic separation capability inherent in MPLS Virtual Private Networks (VPNs).

The security of communications applications begins with the nature of the underlying transport used to provide the service. AT&T Telepresence Solution uses AT&T industry-leading MPLS-based VPN service (i.e., AT&T VPN, AT&T Enhanced VPN Service). These VPN services use the network and the traffic separation protocols inherent in the AT&T MPLS network to maintain separation between individual customer traffic, including telepresence traffic, on the network. Traffic separation on the AT&T MPLS-based network occurs without tunneling or encryption through a combination of BGP routing and MPLS label forwarding. In accordance with the RFC2547 standard, a unique virtual routing and forwarding table is assigned to each customer's VPN. VPN membership depends upon logical or physical ports entering the VPN, where a unique route distinguisher (RD) is assigned to each customer route to make it unique within the MPLS backbone and a unique route target (RT) is assigned to ensure each route is placed into the correct customer virtual routing and forwarding table. A packet received by the AT&T network is associated with a customer's VPN, and a forwarding table associated with the particular VPN is used to determine a set of possible egress interfaces within customer's VPN. In this manner, customer packets from one VPN cannot be forwarded to a different VPN or to a different customer.

AT&T Telepresence Solution customers should thus envision their VPN connectivity as having the following security characteristics, which are derived from the strengths of the AT&T MPLS network on which AT&T Telepresence Solution traffic is carried:

- Containment – Traffic between customer-edge (CE) routers remains within the customer's VPN.
- Isolation – Network design prevents one customer's VPN from materially affecting another customer's VPN.
- Availability – Shared resources are engineered to meet Service Level availability and mitigate denial of services activities through access control lists, filters on learned route and infrastructure hardening.
- Simplicity – IP-based MPLS network VPNs provide a scalable architecture and simplifies provisioning (and hence helps to avoid issues associated with customers having to configure point-to-point solutions, as is the case in IPSec VPN solutions).

Control

AT&T enforces strict operational security controls within the AT&T Business Exchange (Access Control, Filtering, Topology Hiding and Blacklisting).

at&t

The AT&T Business Exchange provides meet-me bridging capability for inter-company (business-to-business), point-to-point telepresence meetings between customer's ATS endpoint(s) and the endpoints of one or more other customers or users who have access to the AT&T Business Exchange, as well as intra-company multipoint connections. To provide security for telepresence calls, AT&T deploys within the AT&T Business Exchange a set of layered, standards-based security policies designed to maintain customer separation and protect service infrastructure.

At Layer 3, AT&T deploys Access Control lists that are applied to each interface (based on service type) to strictly control access to elements within the AT&T Business Exchange and the management infrastructure. Additionally, inbound and outbound route filters are applied to limit route advertisements sent to the customer's domain (based on service type) as well restricting the routes received from the customer domain based on AT&T assigned address space for telepresence units.

AT&T also employs Unicast Reverse Path forwarding which offers a dynamic technique for enabling BCP38/RFC 2827 ingress traffic filtering (anti-spoofing), discarding packets with invalid source IP addresses based on a reverse-path look-up. This is accomplished by checking the FIB (Forwarding Information Base) on the source IP addresses and verifying that the packet is received from a valid source.

At Layer 5, AT&T deploys a business-to-business architecture that uses Session Border Controllers (SBC) to provide topology and address hiding. The SBC acts as a business-to-business User Agreement (B2BUA) within the AT&T Business Exchange providing demarcation of SIP and Media (RTP) to its SBE and DBE respectively. This allows customers to connect to the AT&T Business Exchange without obtaining knowledge of the other AT&T Business Exchange participants' IP addresses or topology. It also prevents direct signaling between the customer domains.

The SBC also serves as a control point to implement security polices designed to protect the AT&T Business Exchange infrastructure from malevolent endpoints. As a part of this function, the SBC monitors signaling traffic and dynamically detects potential attacks and blocks malicious traffic/source attempting to access the network resources. The SBC detects a number of different styles of attacks and dynamically reacts to these attacks by blocking (i.e. blacklisting) the source of the attacks. In order to accomplish these security functions, the SBC monitors:

- Bad Address – SBC blocks endpoints attempting to communicate from addresses that are not configured on SBC. The SBC detects such events when a signaling message is received whose source and destination do not match any configured adjacency.
- Corrupt/Malicious messages – Endpoints sending too many corrupt or unparseable signaling messages may indicate a sophisticated DoS attack aimed at crashing a server or denying service to it. The SBC is designed to detect this event by discovering syntax errors in signaling messages from endpoints as per RFC 4475.
- Authentication Failures – Endpoints sending too many signaling messages for which authentication fails may indicate a DoS attack or a brute force authentication attack. It is detected by SBC when it sends a SIP 401 or 407 error response to an endpoint. This therefore includes both authentication errors generated by the SBC, and also those generated by services accessed through the SBC.
- Routing Failures – Endpoints sending too many signaling messages for which routing fails suggests a random dialer. SBC detects this event when application of local number analysis or routing policy results in a failure of a request. A SIP response is received from a downstream device with an error code of 404, 485 or 604.
- Policy Rejection – If an endpoint is repeatedly being rejected by call admission control policy, it may indicate a DoS attack, or a subscriber deliberately attempting to seriously breach their agreed use to the extent that it will impact other users. SBC detects this event when application of local call admission control policy results in the failure of request.

The detection mechanisms for the above-listed potential attacks use a leaky bucket model with configurable number of occurrence (trigger-size) within the specified time period (trigger-period), so an excessive numbers of the above events occurring within a sufficiently short time period is classed as an attack. When an attack is detected, a block on incoming messages may be placed for the source that is causing the detected events. A block can encompass a range of IP addresses and ports, depending on configuration and the perceived granularity of the attacks. The network management center is notified whenever this occurs, but no notification is made to the blocked endpoint that this has occurred. Dynamic blocks are automatically removed after a configurable timeout interval, but for persistent offenders static manual blocks can be applied.

Security Validation

AT&T Uses Audits and Reviews to Validate Security Compliance

AT&T is committed to using industry-best network security practices, which are reflected in the AT&T Security Policy Requirements (ASPR). The AT&T Chief Security Officer team works with both internal and external auditors to measure the operations and infrastructure compliance with these practices. This is an on-going task that sweeps through all aspects of AT&T's infrastructure – including the MPLS network.

The AT&T processes also include the use of expert reviews and organizational approvals as so-called "Security Gates" applicable to all levels of the organization. For example, AT&T's design and development efforts follow a corporate-wide standard and documented methodology. The ASPR process mandates an expert security review for newly developed processes even at the first conceptualization step and requires approval from designated teams of security experts throughout development. For the MPLS network, this means AT&T conducts:

- Testing – AT&T conducts ongoing intrusion detection, audits and penetration testing against server complexes for network management, customer care and service support. Customer MPLS VPNs are created and configured by an automated provisioning system, and any changes or discrepancies in router configuration, from the backend provisioning database, will be detected by regular discords detection/reports.
- Auditing – On-going audits by independent, internal security teams are used to confirm compliance with the AT&T Security Policy Requirements.
- Reviews – All processes have embedded controls that require expert security reviews.

Security Response

Security Management and Incident Response

With AT&T Telepresence Solution, security management is addressed end-to-end, device by device and flow by flow. As part of this security posture, AT&T uses an active management strategy that incorporates the use of active Intrusion Detection (IDS), Intrusion Prevention (IPS) capabilities and Netflow anomaly detection within the AT&T Business Exchange.

IDS is deployed centrally at the AT&T Business Exchange and is designed to inspect traffic for signature matches based on the latest signature updates. IDS inspects traffic patterns for the latest attacks, and takes action through automation and operations to manage the risk to AT&T and its customers.

Another critical component that AT&T uses in the security management is the capture, monitoring and analysis of traffic flow data to detect trends and anomalies. A "flow" is a Layer 7 concept that consists of session setup, data and session teardown. AT&T collects flow information on traffic as it transverses the AT&T Business Exchange. The Netflow integration takes advantage of anomaly detection using statistical profiling and allows AT&T to detect traffic anomalies.

The information gathered from these devices is fed into a centralized management system which is used by the security team for investigation and forensic analysis. The IDS and IPS systems are continuously updated with security threat signatures as well Security Incident Manager (SIM) to help aid in the diagnosis of potential attacks or threats. The SIM gives a holistic view of the potential attack and correlates all potential threats into incidents. These policies are actively managed by the Network Operations team.

Encryption and Endpoint Authentication

AT&T offers customers the ability to encrypt both media and signaling and to authenticate endpoints for business-to-business calls.

The above-described security policies ensure traffic containment and isolation between customer domains and provide overall protection of the service infrastructure. AT&T Telepresence Solution also provides customers the ability to authenticate and encrypt business-to-business calls.

The AT&T meet-me conference control application is a cornerstone of the AT&T Business Exchange architecture. Unlike the SBC, the meet me conference control application operates mainly on the signaling plane. It routes calls to other devices like the CTMS or the ISR when needed to operate in the media plane. The following is a summary of high level features implemented by this entity in the network.

- Resource Management – The conference control application keeps track of the list of CTMS and ISR resources; monitors these resources; and allows operations personnel to take CTMS/ISR resources in and out of service for maintenance. It also ensures that all ISR and CTMS resources are uniformly used in the service.
- Meeting Validation – The conference control application is responsible for all aspects of meeting management. It implements desired logic that ensures the user has the right meeting PIN; that they are calling within active meeting hours; that allowing the participant to the meeting will not violate participant limits.
- Active Meeting Management – The conference control application is responsible for allocating a free CTMS port if the caller is the first participant to the meeting. In cases where the caller is a subsequent participant, it is responsible for finding the CTMS resource that was allocated to this meeting when the first participant dialed into the meeting and route the call appropriately. It is also responsible for ensuring meeting participants are appropriately disconnected should they continue beyond the end of the 'reserved' duration.
- Call Detail Records – The conference control application generates appropriate CDR records for all calls processed by it for accounting purposes.
- Interface to Web Scheduling System – This interface is responsible for notifying the conference control application of all meeting creation, deletion and modification requests initiated by the end user.

As an additional layer of security, AT&T offers the use of encryption to provide privacy of data and communications for both inter and intra-company point-to-point calls and multipoint CTS to CTS calls, and for guest access participants coming from public networks (Internet, ISDN). To provide privacy during a teleconference call, encryption is applied to both the audio and video streams. Media encryption is enabled with CTMS in compliance to this current model which the CTS endpoints already support. The 509v3 Digital Certificates are used for both signaling encryption (intra-company p2p) and media encryption. DTLS is used to exchange the keys between CTMS and CTS for media encryption. Once the media path is established between the two systems, they initiate a DTLS handshake using their MICs/LSCs to authenticate each other, and then over the DTLS encrypted session they negotiate the sRTP keying material. SRTP then provides the transport for authenticated and encrypted media using HMAC-SHA-1 for authentication and AES-128-CM for encryption.

For more information contact your AT&T Representative or visit us at www.att.com/telepresence.

02/03/12 AB-1643-01