TELE PRESENCE

Security Whitepaper

Vu TelePresence™ is a High Definition video conferencing system that allows users to talk and collaborate within and between companies easily. Given the critical nature of the system especially as it is used by key business executives to make decisions, it becomes very important to keep the system away from hacker attacks and make the system secure. Security within the Vu TelePresence™ solution is handled at multiple levels and more features being added in subsequent releases.

The Vu TelePresence™ unit runs a firewall on-board which blocks out all inbound and outbound ports that explicitly are not required for communication. This helps securing the system from hostile users. No inbound connections via Telnet or SSH are possible. Support is initiated by the user by connecting to a Reverse SSH server and then it is disconnected once the support process is complete. Within the support shell the support staff has access to only a restricted shell and no access to the data within the system which is stored on an Encrypted File system.

The Vu TelePresence™ system uses the XMPP protocol to communicate with peers and accept/reject contact requests. The XMPP system is used during the call setup and call teardown phase. The connection to the XMPP server is using a SSL connection with certificate exchange that verifies the authenticity of the server and does not allow for a “Man-in-the-Middle” attack. The servers are hosted in secure data centers across the United States. Since the connection is over SSL the message content is encrypted using the X.509 standard . Customers can, (at an additional charge) request for a signaling server on premises, which will ensure that all units communicate through the on-site signaling server.

The actual audio/video data between systems flows across the network using the standard RTP protocol. In case customers need a secure conversation; then one can use SRTP and SRTCP[1] .
SRTP allows the conversations to be encrypted and prevents replay attacks. For encryption and decryption of the data flow (and hence for providing confidentiality of the data flow), SRTP (together with SRTCP) utilizes AES as the default cipher. Vu TelePresence™ uses the Segmented Integer Counter Mode. This is a typical counter mode, which allows random access to any blocks, which is essential for RTP traffic running over unreliable network with possible loss of packets. In the general case, almost any function can be used in the role of "counter", assuming that this function does not repeat for a long number of iterations. But the standard for encryption of RTP data is just a usual integer incremental counter. AES running in this mode is the default encryption algorithm, with a default encryption key length of 128 bits and a default session salt key length of 112 bits. To authenticate the message and protect its integrity, the HMAC-SHA1 algorithm (defined in RFC 2104) is used, which produces a 160-bit result, which is then truncated to 80 or 32 bits to become the authentication tag appended to the packet. The HMAC is calculated over the packet payload and material from the packet header, including the packet sequence number. To protect against replay attacks, the receiver maintains the indices of previously received messages, compares them with the index of each new received message and admits the new message only if it has not been played (i.e. sent) before. Such an approach heavily relies on the integrity protection being enabled (to make it impossible to spoof message indices).

[1]: Release planned on December 2010 timeframe