Technical Note:

Security Considerations for Educational Services Platform

Connectivity's Educational Services Platform infrastructure is a 'State of the Art' system of technologies based on proprietary, open source and licensed components.

At a glance

- AES-256 bit media encryption
- HTTPS with certification login
- TLS with certification for signaling
- New component blocking for spoof prevention
- Encrypted token technology for session security
- No login information kept at the desktop
- Secure Firewall Traversal

User Login and Inter-Component Signaling

With SSL security enabled the system automatically establishes an encrypted HTTPS channel with each endpoint that attempts to access the system and performs certificate exchange, issued by third party certifying authority. Once certificate verification is completed, login and password information is transmitted securely to the system over the same encrypted HTTPS channel.

For the client/server application signaling, TLS is employed with key exchange taking place over secured TLS connections and support for the same certificate process as HTTPS.

Media Encryption

To ensure that the content of your session cannot be intercepted and decoded without your knowledge, the system employs AES-256 bit encryption over SRTP for audio, video and shared content. A set of keys is used for each form of media for each leg of the conference. The conference router decrypts and re-encrypts each media stream as it passes through for unprecedented security from one endpoint to the other over public networks.

Component Authentication (Spoof Prevention) & Session Security

Each component in the conferencing system has a unique identifier which is communicated to the system over a secure link and is otherwise not accessible. New components added to the network go to the system for configuration. If no configuration is defined for that machine's specific ID, the machine is blocked from joining the network until the administrator accepts and configures the component.

On the client side, a unique token is generated and encrypted by the system and sent to the *endpoint* at login over a secured link after the endpoint has sent the system its unique identifier. The encrypted token is stored by the endpoint and the session is kept alive until the next time the user successfully logs in. Each time the endpoint attempts to access the system for services (such as call initiation), the endpoint presents its session token, ensuring that the endpoint is in fact the machine where the credentialed user last logged in.

Secure Firewall Traversal

Connectivity provides methods of secure firewall traversal, enabling organizations to leverage the public network to provide connectivity for mobile end users without compromising the integrity of the private network or requiring additional expensive equipment. For implementations where the necessary range of UDP ports are opened on the network, the client uses industry standard ICE/STUN to negotiate UDP ports with the system. These same protocols are employed for NAT traversal.

For implementations where the UDP ports are closed on the network, a proxy solution overcomes these blocking issues in a secure fashion by tunneling on port 443 using industry standard TCP. The client is able to auto-detect if firewall blocking is taking place and automatically switch to proxy configuration as needed and supports existing hardware-based web proxies.