grouptalk

Introduction

GroupTalk is a service for Push-to-Talk (PTT). Smartphones, PC:s and two-way radios with RoIP interfaces can connect to the service. This document discusses GroupTalk security aspects.

Clients

The following clients are currently available:

- Web browser (for administration)
- GroupTalk for Android (mobile app)
- GroupTalk for iOS (mobile app)
- GroupTalk Dial-in for Android
- GroupTalk for PC (Java webstart app)
- GroupTalk Web Dispatcher (HTML5)

Password Management and Authentication

Users need a password to access GroupTalk web administration and to connect using the PC client. Optionally, password may also be used when connecting using the mobile client. Passwords are stored by GroupTalk in a hashed format (salted to prevent dictionary attacks). There is no known practical way of retrieving the plaintext password. To set or change the password for a user either access to the email account specified for the user or web administrator access for the users company is required. Password resets are handled by requesting a long, random token to be sent to the users email address. The token is only valid for a short time (a few hours) and is required to set a new password.

For smartphone users with the GroupTalk app there is an alternative way of authenticating by using a long, device-specific random token, generated server-side and transferred to the client in separate parts using both SMS and IP. This token cannot be used for web login, and must be refreshed periodically according to company policies.

For the Dial-in mobile app authentication is needed both for syncing of contacts and when dialing into the service. The contact sync is done over HTTPS using a token sent in an SMS to a phone number previously configured for the user. Authentication when dialing in is based on whitelisted caller id (the same configured phone number used for the SMS).

Firewall Settings

GroupTalk mobile clients and PC Java client connects to a GroupTalk server through a single, persistent TCP connection, using a proprietary protocol. The connection is always initiated by the client. The client uses DNS to determine server IP:s and ports. The firewall is required to allow outgoing TCP connections to ports 10207-10214 on 88.80.181.10 corresponding to multiple GroupTalk servers with ports for both unencrypted and encrypted communication. The port range may be expanded in the future.

Type:	PTT client access
Port range:	10207-10214 (TCP+UDP)
IP:	88.80.181.10
Direction:	outgoing connections

Besides the persistent TCP connection a transient UDP connection is needed for transmission of audio. The UDP connection is also always initiated by the client and server port range and IP is the same as for the TCP

connection (e.g. if the client is connected to the server via TCP on 88.80.181.10:10209 the UDP packets will be sent to and received from 88.80.181.10:10209). Thus, the firewall needs to open the same ports for UDP as for TCP. If the firewall is using NAT it must be symmetric. The firewall needs to keep UDP sessions open for at least 20 seconds after the last packet sent from the client to the server. This behavior is default for most firewalls.

Type:	web access
Ports:	80 and 443 (TCP)
IP:	88.80.181.10
Direction:	outgoing connections

For web admin access the standard HTTP and HTTPS ports must be opened for outgoing connections. The HTTP port is not required, but is convenient as it redirects the user to HTTPS.

Type:	web dispatcher
Ports:	443 (TCP)
IP:	88.80.181.10-12
Direction:	outgoing connections

The GroupTalk Web Dispatcher uses the same HTTP and HTTPS port as the web admin, but also needs HTTPS ports for additional IP addresses. The web dispatcher does not use UDP for audio, instead tunneling it through the HTTPS connection.

Security Options

Roles

Users may be assigned one or multiple roles. A role grants the user permission to use the system accordingly. The roles are

- Dial-in: the user is permitted to call into the GroupTalk system from a phone with a number specified for this user
- PC PTT: the user may use the PC client and web dispatcher to access GroupTalk
- Mobile PTT: the user may use the mobile app to access GroupTalk
- Web roles
  - None: the user may change his password, but not login to the web admin
  - Basic: the user may login and change his password
  - Reader: the user may view statistics and status in addition to the basic role
  - Admin: the user may administer the service for the company (users, radio interfaces etc) in addition to the reader role

Access restrictions

To further increase security GroupTalk access can be restricted to specified networks, i.e. PC clients and web logins can be limited to users on the corporate network, while mobile access can be allowed from a mobile network associated with a corporate APN.

Password changes

A company may decide to force users to change passwords regularly. If this feature is used, reminders to change password are sent out to the user before the password expires. Old passwords are stored and users cannot reuse old passwords.

Encryption

All access to the web administration interface uses the HTTPS protocol with standard SSL encryption. The same encryption is also used (if enabled) for the persistent TCP connection for mobile, PC client and web dispatcher access. The UDP audio stream is encrypted using AES-256 with a per session generated key, transmitted over the SSL encrypted TCP connection. In addition, all packets are hmac authenticated to prevent forged or modified packets. Packet counters are used to prevent replay attacks.

Server Environment

The GroupTalk service is running on virtual servers on hardware located in Gothenburg, using GothNet for co-location. It runs on SELinux (Security Enhanced Linux) with a high level of redundancy. The internet connection is provided by Telenor.