

IBM® Lotus® Sametime® 8 security features

Smriti Talwar

IBM Software Group
Lotus Sametime Security Architect
Mulhuddart, Ireland

Gili Revel

IBM Software Group
Lotus Sametime Development Lead
Haifa, Israel

May 2009

© Copyright International Business Machines Corporation 2009. All rights reserved.

Abstract: This white paper describes the security features of IBM® Lotus® Sametime® 8.0 software, including a discussion of authentication and encryption for each of the major functional units of Lotus Sametime.

Contents

1	Lotus Sametime security features.....	3
1.1	Sametime community server.....	3
1.2	Virtual Places.....	3
1.3	Authentication.....	3
1.4	SPNEGO support.....	5
1.5	Encryption.....	6
1.6	Authentication sequence.....	6
1.7	Ports used by community services.....	7
1.8	HTTP , Domino, LDAP, and Sametime intraserver ports.....	8
2	Sametime Meeting Server.....	9
2.1	Authentication.....	9
2.2	Encryption.....	9
2.3	Meeting services ports.....	10
2.4	Recorded meeting broadcast services ports.....	11
2.5	Audio/video services ports.....	12
3	Lotus Sametime Gateway.....	12
3.1	Authentication.....	12
3.2	Encryption.....	13
4	Lotus Sametime Advanced software.....	13
4.1	Authentication.....	13
4.2	Access control.....	13
5	Lotus Sametime Unified Telephony.....	14
5.1	Authentication.....	14
5.2	IP telephony signaling.....	14
5.3	IP telephony media.....	14
5.4	Encryption.....	14
6	Lotus Sametime Mobile software.....	15
6.1	Authentication.....	15
6.2	Encryption.....	15
7	Lotus Sametime integration with Microsoft Office.....	15
7.1	JNI based.....	15
7.2	Meeting integrator.....	16
7.3	STHelper.....	16
8	HTTP tunneling on port 80.....	17
9	Lotus Domino database encryption.....	17
10	FIPS support.....	17
11	Directory support.....	18
12	Resources.....	18
13	About the authors.....	18

1 Lotus Sametime security features

IBM Lotus Sametime Standard software is a client--server application that enables a community of users to chat and collaborate in real time, and hold online meetings over an intranet or the Internet.

1.1 *Sametime community server*

In Lotus Sametime software, the community server, in conjunction with several other server applications, provides services such as presence awareness, instant messaging, and places. It provides these services using the Virtual Places (VP) protocol, a proprietary protocol unique to Sametime.

The community consists of:

- Clients who are connected using TCP/IP
- Multiplexers that improve Sametime scalability by I/O concentration
- Community hubs that log in Sametime clients, route messages between members, and notify subscribers of events in the community
- Server applications that are connected to community hubs using TCP/IP

This server handles log-in requests, and the multiplexers handle connections from clients that access the Sametime server through a direct TCP/IP connection, or HTTP, HTTPS, or a SOCKS proxy.

1.2 *Virtual Places*

VP is the name of the binary protocol that is used for communication between all the components in Lotus Sametime. This communication is done via channels, which are virtual connections between two community entities.

A channel is responsible for defining the routing path between the two end points of the channel, ensuring the correct order of messages, and supplying notifications when a network connection along the path is broken.

Upon connecting to the community, a default master channel is created between a community participant and its serving community hub. Other channels can be created by use of the master channel. When a client connects to a service in the community or interacts with another user, a channel is created for the interaction.

As an example, the route from the client to the buddylist server application uses the master channel between the client and the community server and then uses the channel between the community server and the buddylist server application.

1.3 *Authentication*

Here we discuss some aspects of authentication.

1.3.1 *Client-to-server connections*

Sametime Connect clients access Sametime services by opening a socket connection to a Sametime multiplexer. The clients connect to the Community Services multiplexer

and not to the Sametime server, freeing the Sametime server from the burden of managing live client connections. The multiplexer is dedicated to this task.

The Community Services multiplexer maintains a single IP connection to the server, and the data from all Community Services clients is transmitted over this IP connection to the Community Services on the Sametime server.

1.3.2 Types of authentication

Lotus Sametime has two types of authentication:

- Basic password authentication
- Authentication by token

Basic password authentication. Users must provide credentials to the Sametime Connect client, which connects to the Community Services on the server. When logging on to Sametime, users must use their credentials stored in the IBM Lotus Domino® directory.

If Lotus Sametime has been configured to operate with an LDAP directory, it authenticates users based on the user names and passwords stored in the LDAP directory and uses the respective bind API, depending on the directory used.

Authentication by token. Sametime supports two types of tokens: LTPA (Lightweight Third-Party Authentication) and ST (secret token).

- **LTPA token:** The LTPA token is created to authenticate users for single sign-on (SSO) and contains the name of the user who has been authenticated. When Lotus Domino creates an LTPA token, it places the distinguished name of the user in the token by default. This scenario typically occurs in user configurations where there are multiple directories used by various servers participating in SSO.
- **ST token:** The secret token can be created by the Secrets and Tokens authentication databases, the Domino SSO feature or both. This token can be generated by Sametime using the authentication databases or the Domino SSO feature.

1.3.3 Server-to-server connections

There are many cases in which a server component must connect to another, including, for example, server-to-server, server-to-multiplexer, and server application-to-hub connection.

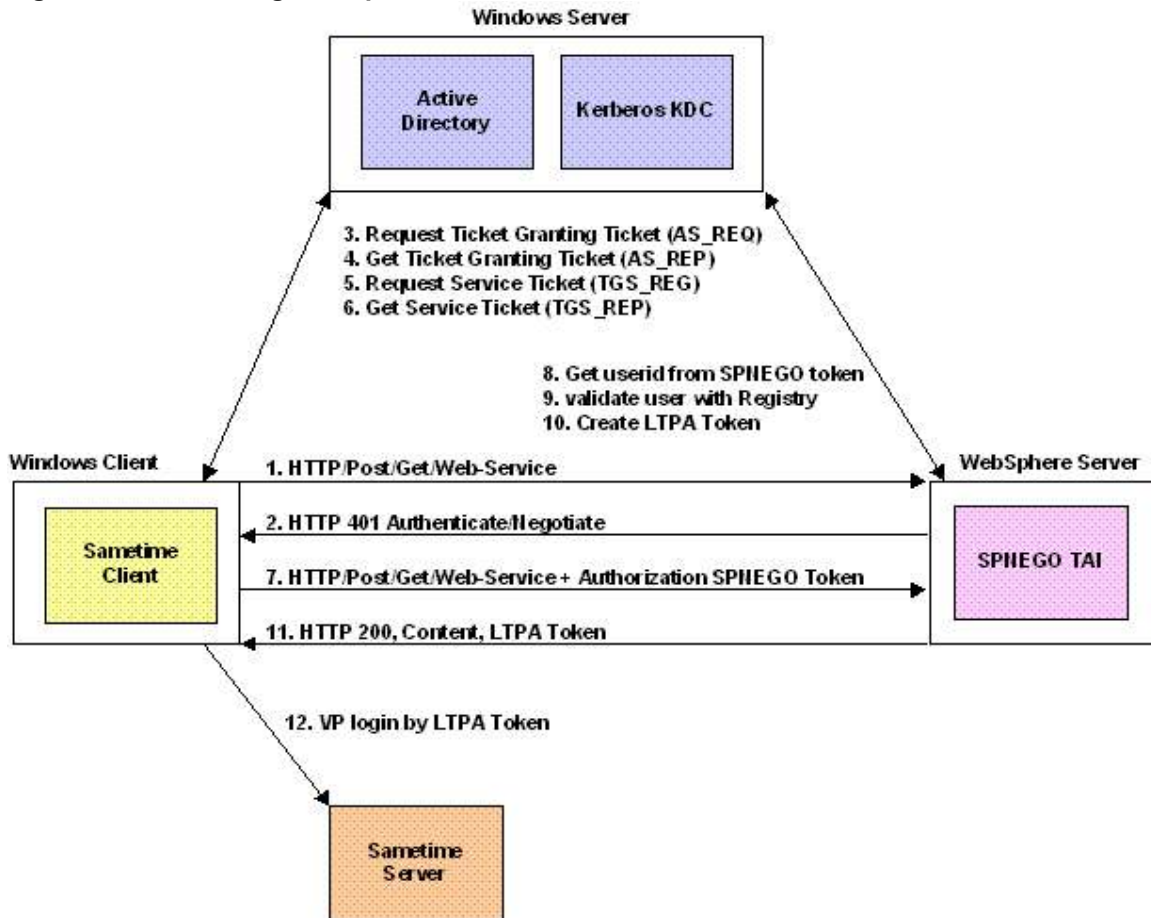
We can authenticate these connections by checking the IP address from which the connection originates and ensuring that the address is listed in the Allowed IPs configuration list (configured in Lotus Domino).

1.4 SPNEGO support

We can also configure the Sametime client for SSO by using the Simple and Protected GSS-API Negotiation Mechanism (SPNEGO). Client authentication is done via Microsoft® Active Directory, and the LTPA token is issued by IBM WebSphere® Application Server.

This feature lets Sametime users log in and authenticate only once at their desktop and thereafter automatically authenticate with the Sametime server. Figure 1 shows the SPNEGO log-in sequence.

Figure 1. SPNEGO log-in sequence



After logging into the Active Directory domain on a Microsoft Windows® desktop, users can start the Sametime Connect client. When they click Log In, a two-phase log-in operation begins

In phase 1, the client executes an HTTP request for a protected URL on WebSphere Application Server. This request is processed by the SPNEGO trust association interceptor (TAI), which triggers the SPNEGO negotiation between the client system and WebSphere Application Server. After trust is established, an LTPA token is sent to the

client in the HTTP response. In phase 2, the client securely logs into the Sametime server using the LTPA token.

1.5 Encryption

Encryption is handled via RC2 with a 128-bit key, and keys are generated by use of Diffie-Hellman for each logical channel in use. There can be many logical channels in use on a single TCP connection. Logical channels are used in the cases of communication from:

- Client to server, as in the authentication example above.
- Client to client, using the server as an application-layer router, as in the case of instant messaging.
- Server to server, to satisfy the requirements of distributed processing and clustering.

In all the above scenarios, the data is fully encrypted.

1.6 Authentication sequence

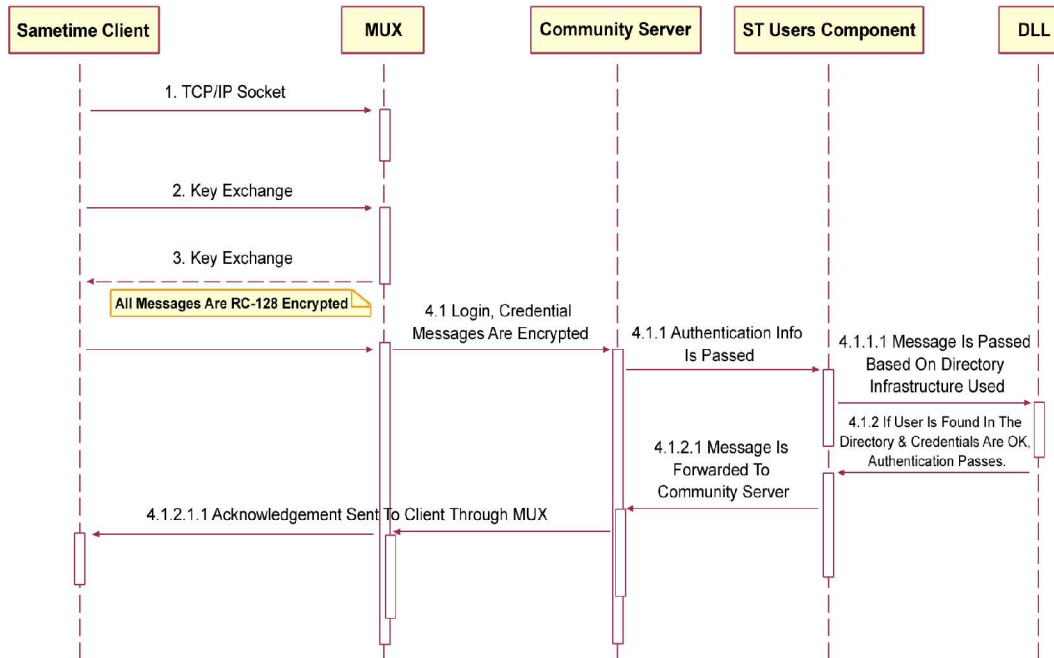
During the handshake phase, when the client initiates a connection to the multiplexer, they also agree on a shared key, using the Diffie-Hellman key agreement method.

Subsequently the multiplexer agrees on another secret key with the server. Messages sent from the client to the multiplexer are encrypted and decrypted using their agreed upon shared key. Similarly, messages from the multiplexer to the server are encrypted and decrypted using their agreed upon shared key.

When a message is sent from the client to the multiplexer, it is first encrypted at the client and decrypted at the multiplexer. Similarly, the message is encrypted at the multiplexer and decrypted at the server.

Figure 2 outlines the sequence of events that occur when the client goes through the authentication process. This diagram shows the flow of credentials through the various components. After these credentials are verified by the directory infrastructure in use, the server accepts the log-in.

Figure 2. Authentication process



1.7 Ports used by community services

The ports listed in Table 1 are used by the Lotus Sametime community services and most are configurable.

Table 1. Sametime community services ports

Default port number	Purpose
1516	Community services listen for direct TCP/IP connections from the community services of other Sametime servers on this port. The multiplexer and other Sametime applications connect on this port.
1533	Community services listen for direct TCP/IP connections and HTTP-tunneled connections from the community services clients (such as Sametime Connect and Sametime Meeting Room clients) on this port. Community services also listen for HTTPS connections from the community services clients on this port. The community services clients attempt HTTPS connections when accessing the Sametime

	<p>server through an HTTPS proxy server. If a community services client connects to the Sametime server using HTTPS, the HTTPS connection method is used, but the data passed on this connection is not encrypted.</p>
80	<p>If the administrator allows HTTP tunneling on port 80 during the Sametime installation, the community services clients can make HTTP-tunneled connections to the Community Services multiplexer on port 80.</p> <p>If the administrator does not allow HTTP tunneling on port 80 during the Lotus Sametime installation, the Domino HTTP server listens for HTTP connections on this port.</p>
8082	<p>When HTTP tunneling support is enabled, the community services clients can make HTTP-tunneled connections to the community services multiplexer on port 8082 by default.</p> <p>Community services clients can make HTTP-tunneled connections on both ports 80 and 8082 by default.</p>

1.8 HTTP , Domino, LDAP, and Sametime intraserver ports

The ports in Table 2 are used by the Sametime services, HTTP services, Domino application services, and LDAP services.

Table 2. Sametime HTTP, Domino application, and LDAP services ports

Default port number	Purpose
80	<p>If the administrator allows HTTP tunneling on port 80 during the Sametime installation, the Community Services multiplexer on the Sametime server listens for HTTP connections from Web browsers, Sametime Connect clients, Sametime Meeting Room clients, and Sametime Recorded Meeting clients on port 80.</p> <p>If the administrator does not allow HTTP tunneling on port 80 during the Sametime installation, the Domino HTTP server listens for HTTP connections on this port.</p>
Alternate HTTP port 8088	<p>If the administrator allows HTTP tunneling on port 80 during the Sametime installation (or afterward), the Domino HTTP server on which Sametime is installed must listen for HTTP connections on a port other than port 80.</p> <p>The Sametime installation changes the Domino HTTP port from port 80 to port 8088, if the administrator allows HTTP tunneling on port 80 during a Sametime server installation.</p>

389	If the Sametime server is configured to connect to an LDAP server, the Sametime server connects to the LDAP server on this port.
443	The Domino HTTP server listens for HTTPS connections on this port by default.
1352	The Domino server on which Sametime is installed listens for connections from Lotus Notes® clients and other Domino servers on this port.

2 Sametime Meeting Server

The meeting services provided by Sametime Meeting Server support multimedia conferencing, including audio and video, and have built-in support for the recording of meetings and their subsequent playback. These services are accomplished with a combination of standard and proprietary protocols.

This server provides communication software that supports screen sharing and whiteboard data between multiple users in a meeting. The services also maintain lists of active, scheduled, and completed meetings and are responsible for starting and stopping instant and scheduled meetings.

2.1 Authentication

When a multimedia activity is added, the meeting room client makes a meeting connection to the server. This connection is authenticated via a token that is acquired by use of the community token service. The client and server use the same Diffie-Hellman method to agree on a secret key, which is then used to encrypt the authentication token that is sent to the server.

In addition, there's an option that lets users specify a meeting password for a meeting when creating a new meeting. A meeting password is valid only for one meeting and applies only to that meeting, unless it's a recurring meeting. The user creating the meeting password must notify other participants about the meeting password before the meeting starts. This option is also encrypted via the negotiated key before being sent to the server.

Users can also restrict access to a meeting by entering the names of users in a Restrictions list when creating a meeting. Only users who are selected in the Restrictions list are allowed to access the meeting. This level of meeting security is controlled by the user who creates the meeting.

2.2 Encryption

The main protocol used by a meeting client is based on T.120. As with T.120, each message contains two parts, the routing header and the application data. The routing header is sent in the clear and is used by the server to determine how to handle each message. There is no user-specific information in this part of the message.

The application data contains everything that is related to the content of the meeting. When encryption is enabled for a particular meeting, then the entire application data section is encrypted.

After a connection is successfully authenticated, and a user is permitted into a meeting, the server sends to that user an encryption key that is specific to that meeting. All subsequent messages are encrypted using this key.

Because the server gives the same key to every user in the meeting, it is not necessary for the server to decrypt and re-encrypt any messages before passing them on. In this way, encryption is end-to-end within a meeting, and the server needs only the routing headers to determine what to do with a message.

Note that encryption is handled via RC2 with a 128-bit key.

2.3 Meeting services ports

The default ports in table 3 are used by the Sametime meeting services. These ports are configurable.

Table 3. Meeting services ports

Default port number	Purpose
8081	Meeting services listen for the Sametime protocol over TCP/IP connections from the meeting room client on this port. The screen-sharing whiteboard components of the Sametime meeting room client exchange data with the server over this connection. Send Web page and question-and-answer polling use the community service protocols.
80	If the administrator allows HTTP tunneling on port 80 during the Sametime installation, the meeting room client can make HTTP-tunneled connections to the Community Services multiplexer on port 80.
1503	Meeting services listen for T.120 connections from the meeting services of other Sametime servers on this port. If multiple Sametime servers are installed, this port must be open between the two servers for the servers to exchange screen-sharing, whiteboard, and other meeting services data.
1516	In a multiple Sametime server environment, a single meeting can be simultaneously active on multiple Sametime servers. This functionality is sometimes called "invited servers." The community server port 1516 must be open between two Sametime servers to enable one server to extend a meeting invitation to another server in support of the invited server's functionality.

9092	The event server port on the Sametime server is used for intraserver connections between Sametime components.
9094	The token server port on the Sametime server is used for intraserver connections between Sametime components.

2.4 Recorded meeting broadcast services ports

The default ports in table 4 are used by the Sametime recorded meeting broadcast services. These ports are configurable.

Table 4. Recorded meeting broadcast services ports

Default port number	Purpose
554	Recorded meeting broadcast services listen for Real-Time Streaming Protocol (RTSP) call-control connections over TCP/IP on this TCP/IP port. RTSP uses TCP as the transport service. The recorded meeting client can make the RTSP TCP/IP connection directly to the recorded meeting broadcast services or through a SOCKS proxy server. This port is specific to IBM AIX®, Linux®, and Sun Solaris.
80	If the administrator allows HTTP tunneling on port 80 during the Sametime installation, the recorded meeting clients can make HTTP-tunneled connections to the Community Services multiplexer on port 80.
Dynamic UDP ports	Recorded meeting broadcast services stream meeting data in RTP format from the server to the client over UDP ports. The specific UDP ports are chosen randomly by the recorded meeting client and cannot be controlled by the administrator. NOTE: Recorded meeting broadcast services can also stream audio and video data to recorded meeting clients. A meeting might include three separate streams, one each for audio, video, and screen-sharing/whiteboard data. If the client or server network, or any network between the Sametime server and the client, does not allow UDP traffic, then the recorded meeting broadcast services tunnel the streamed data over the initial RTSP TCP/IP control connection that occurs on port 554.
8083	Recorded meeting broadcast services use this port for internal control connections between its components. This port should be changed only if another application on the Sametime server is using port 8083.

2.5 Audio/video services ports

The following default ports table 5 are used by the audio/video services. These ports are configurable.

Table 5. Audio/video services ports

Default port number	Purpose
8081	The Sametime meeting room client establishes a TCP/IP connection with the meeting services server on this port. The audio/video services and the audio/video components of the meeting room client use this connection to the meeting services for call-control functions.
49252 to 65535 Dynamic UDP port range	Audio/video services listen for inbound audio and video streams from Sametime meeting room clients on a range of UDP ports specified by the administrator. The UDP ports are selected by the audio/video services dynamically from within the range of ports specified by the administrator.
8084	If UDP is unavailable between a Sametime meeting room client and a Sametime server, Sametime uses this TCP port when attempting to tunnel the RTP audio and video streams using the TCP transport.
9093	Interactive audio/video services use this port for internal control connections between its components. This port should be changed only if another application on the Sametime server is using port 9093.

3 Lotus Sametime Gateway

The Lotus Sametime Gateway allows a Sametime community to interoperate with other instant messaging communities using Session Initiation Protocol (SIP; with SIMPLE extensions) or Extensible Messaging and Presence Protocol (XMPP). This includes access to several of the public IM communities, including AOL, Yahoo!, and Google.

Users in a Sametime community can add users from other communities to their buddy lists, and vice versa, and can chat with users in other communities. Sametime Gateway does not allow Session Initiation Protocol (SIP) or XMPP clients to log in; only connections from other SIP or XMPP servers are accepted. Furthermore, the Sametime administrator can control with which remote communities to interact.

3.1 Authentication

As mentioned above, the Sametime gateway does not allow clients to connect, so user-level authentication is not an issue. The Transport Layer Security (TLS) provides

security features to SIP and XMPP connections to other servers, as specified in the respective standards.

3.2 Encryption

There are two sides to the gateway: The side facing the Sametime community, which proxies internal access to clients in other communities; and the side facing the remote servers, which proxies external access to clients in the Sametime community.

On the Sametime side, encryption is handled exactly as described above for all other clients and servers. On the SIP/XMPP side, encryption is handled by requiring TLS connections to remote servers. Connections to Google Talk servers over XMPP cannot use TLS; instead, they rely on TCP/IP. There is no control over how encryption is handled after data is transferred to a remote server.

The connection between the local Sametime community server and its Sametime gateway server uses the proprietary Virtual Places (VP) protocol.

4 Lotus Sametime Advanced software

IBM Lotus Sametime Advanced software enhances the use of real-time collaboration by adding advanced personal, team, and community collaboration capabilities. Some of the features included are persistent group chat, broadcast tools, screen sharing, and location services.

4.1 Authentication

Clients can access this application using the Web user interface or the Sametime client.

The Web interface uses standard form-based authentication, which uses Base64 encoding, so unless this interaction is over SSL, the username and password are exposed. All subsequent requests to the server are authenticated using the LTPA token.

The Sametime client uses Simple Object Access Protocol (SOAP) to communicate with the advanced server; the credentials in this case are also Base64 encoded.

The broadcasting feature available in Sametime Advanced software is built on the WebSphere Event Broker's publish/subscribe capability. WebSphere Event Broker is used for the distribution and routing of messages from disparate applications.

WebSphere Event Broker supports multiple transport protocols and extends the flow of information in an organization beyond point to point, using flexible distribution mechanisms such as publish/subscribe and multicast. Credentials are passed to the Event Broker without encryption, so it's essential to use SSL in the deployment to ensure security.

4.2 Access control

Sametime Advanced software allows access control both at the application level and the feature level. The integrated solution console can be used to specify security roles for users or groups at the application level.

At the feature level, you can edit roles within the application by modifying role settings available in broadcast communities, chat rooms, and folders. You can control access at the feature level by editing role settings in the broadcast communities, chat rooms, and folders.

5 Lotus Sametime Unified Telephony

IBM Lotus Sametime Unified Telephony software helps integrate heterogeneous back-end telephone systems. It offers users click-to-call or click-to-conference capabilities from within the Sametime client, the Lotus Notes client, or a Microsoft Office application.

It lets users make phone calls on a built-in softphone to save time and reduce telephony costs, while also streamlining the call management process with incoming call alerts, robust call management, and automated call routing to any designated phone line.

5.1 Authentication

The Sametime Unified Telephony client is essentially the Sametime Connect client with the unified telephony plug-in, and it uses the same authentication mechanism as the standard Sametime client. In addition, the SIP softphone must be registered with the SIP proxy/registrar.

SIP authentication with the SIP proxy/registrar is done by use of Lotus Sametime credentials over a TLS secured connection.

5.2 IP telephony signaling

SIP is used for setting up the communication session for Sametime Unified Telephony, which supports both basic and digest authentication, both of which are used with the user's community server credentials.

5.3 IP telephony media

Secure Real-time Transport Protocol (SRTP) is used for media transport in Sametime Unified Telephony. SRTP provides confidentiality, message authentication, and replay protection to media traffic, such as audio and video. The protocol does the following:

- protects the user from eavesdropping, packet spoofing, and message replay
- offers increased security by providing confidentiality for RTP by encryption of the payloads
- achieves integrity for the RTP packets along with replay protection
- has an extensible framework that permits upgrading to new cryptographic algorithms
- provides security for unicast and multicast applications

5.4 Encryption

There are two types of encryption relevant here.

5.4.1 IP telephony signaling

SIP TLS is supported. Transport Layer Security encrypts SIP signaling traffic, guaranteeing message confidentiality and integrity. IP security (IPSec) is a network-

security mechanism that provides Transport Layer Security.

5.4.2 IP telephony media

SIP by itself does not consider the encryption of media data; instead, it provides media stream security through the use of SRTP. Session Description Protocol (SDP) is used for key management.

Sametime Unified Telephony supports SRTP via SDP and Security Descriptions for Media Streams (SDES). The Sametime Unified Telephony client uses the same mechanism as the standard Sametime client because, again, it is basically the client with the unified telephony plug-in.

6 Lotus Sametime Mobile software

IBM Lotus Sametime Mobile software is the Sametime client that runs on mobile devices including Microsoft Windows Mobile, BlackBerry, Sony Ericsson, and Nokia devices. Sametime Mobile uses the HTTP-based Sametime links protocol to communicate with the Sametime server.

6.1 Authentication

Sametime Mobile requires that you enter the Sametime user ID and password to log into the server. Typically in mobile devices, you also use a virtual private network (VPN) to get access to the network on which the Sametime server resides. Use of a VPN also requires authentication, which varies based on the VPN used.

In addition to a VPN, Sametime Mobile can use HTTPS and a reverse-proxy SSO configuration to access the Sametime server. The user can set the details of this proxy (proxy URL, port, credentials) in the Sametime Mobile settings.

6.2 Encryption

Sametime Mobile uses 128-bit RC2 encryption for messages over the Sametime links protocol. Additional encryption is added when a VPN or HTTPS reverse proxy is used to access the Sametime server.

7 Lotus Sametime integration with Microsoft Office

The functional categories used for Microsoft Office integration are:

- JNI based
- Meeting integrator
- STHelper

7.1 JNI based

There are two functions available in the Sametime client that use JNI to access Microsoft Outlook: Autostatus reads the Outlook calendar and updates the Sametime presence status as required, while chat history writes transcripts into the Microsoft Outlook mail repository.

The authentication and authorization scheme in both the functions is driven entirely by Outlook. If Outlook is not already running when the Sametime feature is used, Outlook is launched and presents the user with its log-in dialogs.

If Outlook is already running when the Sametime feature is invoked, it automatically uses the currently running user account for all interactions with Lotus Sametime.

7.2 Meeting integrator

Meeting integrator is a feature that installs into Outlook. This feature creates Sametime meetings that correspond to Outlook meetings that the user creates. There is an option to set a password for the Sametime meeting, when a new meeting request is created.

The meeting integrator uses an add-in DLL that checks the invite form. When a Sametime meeting is desired, the DLL has a direct conversation with the meeting server, using a service API (in version 8.0.2, a REST API) running in an HTTPS servlet on the server.

Basic authentication is supported here; therefore, an HTTPS connection must be used with the meeting server.

7.3 STHelper

This section covers the other Microsoft Office integration features, like the toolbars seen in Outlook and Office applications, smart tags, and the SharePoint integrator. They interact with the Sametime client via STHelper.

The STHelper is a COM object that exposes a simple API to its consumer. It is used to resolve requests when an e-mail is selected in Outlook or when the chat button is invoked from the Outlook toolbar.

The second logical component of STHelper is a Remote Procedure Call (RPC) communication channel to the locally running Sametime Connect client. The RPC channel uses MicroBroker, a publish/subscribe bus available in the IBM Lotus Expeditor platform on which the Sametime client is built.

The MicroBroker itself resides in the Java UIM application as part of an Eclipse feature called Brokerbridge. STHelper uses a set of MicroBroker C libraries to connect to a MicroBroker running on localhost port 51833. As a security measure, the MicroBroker is configured to permit connections only from the local system.

The actual exchange of data on the channel is by XML and is not encrypted. The general operation of features runs against the currently logged-in Sametime user over at the client. To prevent SPIM (spam over instant messaging), the STHelper consumer can perform only the first-stage initiation of an action; user interaction is usually required to complete the action.

For example, STHelper cannot entirely drive a chat with another user; it can open the local chat window intended for a target buddy and enter the first line of text, but the local user still needs to send the message to the target.

8 HTTP tunneling on port 80

If the Sametime server has been extended to Internet users, the configuration of a remote client's firewall might prevent the client from connecting to the Sametime server.

For example, to exchange presence and chat data with other clients in a meeting, a Sametime client connects to the community services on a Sametime server using TCP/IP port 1533 (by default). To exchange screen-sharing and whiteboard data, a Sametime client connects to the meeting services using TCP/IP port 8081 (by default).

Many firewalls allow only HTTP connections on port 80 and block the connection attempts that occur on ports 1533 and 8081. To establish connections in these environments, Sametime clients can automatically attempt a connection using HTTP tunneling over port 80. Using this tunneled connection, Sametime clients are able to communicate with the community services, meeting services, or recorded meeting broadcast services.

9 Lotus Domino database encryption

The information created and maintained in Lotus Domino databases via the operation of Sametime features could be confidential for an organization; for instance, the schedule of meetings maintained in STCenter.nsf.

In this case, both Domino NSF encryption and HTTPS access to Lotus Domino Web server functions should be used. The access to the Domino Web server would use SSL, which provides communications privacy and authentication for Domino server tasks that operate over TCP/IP.

SSL offers these security benefits:

- Data is encrypted to and from clients, so privacy is ensured during transactions
- An encoded message digest accompanies the data and detects any message tampering
- The server certificate accompanies data to assure the client that the server identity is authentic
- The client certificate accompanies data to assure the server that the client identity is authentic

10 FIPS support

Lotus Sametime supports the U.S. government-defined security requirements for cryptographic modules known as FIPS 140-2 (Federal Information Processing Standard 140-2).

The preferred design approach for FIPS compliance is using the IBM cryptographic libraries ("SSLite" and "CryptoLite") to establish TLS connections between clients and the server and to encrypt the UDP data.

To maintain FIPS 140-compliance for all data exchanged between clients and the Sametime server, installation of a FIPS proxy device is needed on WebSphere Application Server to accept data on behalf of the Sametime server

Also, because the Domino HTTP server is not FIPS 140-compliant, an IBM HTTP server must be deployed as a proxy for the HTTP data to the Sametime server.

11 Directory support

Sametime 8.0 software supports the following LDAP directories:

- IBM Tivoli® Directory Server versions 5.2 and 6.0
- IBM Lotus Domino 6.5, 7.0, and 8.0
- Microsoft Active Directory 2000, 2003
- Sun ONE Directory 5 (iPlanet 5.1 and 5.2)

Note that it's possible to encrypt the connection to the LDAP server using SSL. To apply the SSL protocol you should use the LDAP certificate signed by a certification authority (for example, VeriSign).

12 Resources

- IBM Lotus Sametime 8 information center, [Managing security](#).
- IBM Lotus Notes and Domino information center, [SSL security](#).
- Lotus Security Handbook (an IBM Redbooks® publication):
<http://www.redbooks.ibm.com/redbooks/SG247017/wwhelp/wwhimpl/java/html/wwhelp.htm>
- Digest SIP Authentication, SIP: Session Initiation Protocol:
<http://www.ietf.org/rfc/rfc3261.txt>
- SRTP: The Secure Real-time Transport Protocol:
<http://www.ietf.org/rfc/rfc3711.txt>
- SDES: Session Description Protocol (SDP) Security Descriptions for Media Streams:
<http://www.ietf.org/rfc/rfc4568.txt>

13 About the authors

Smriti Talwar is the Security Architect for Lotus Sametime in IBM's Dublin Software Laboratory. She has 11+ years of design and development experience in domains that include eLearning, social services, financial, CRM, telecommunications and collaborative software. Her current areas of interest are active content security, security in SDLC, risk assessment, and federated identity management. She can be reached at Smriti.Talwar@ie.ibm.com.

Gili Revel is a Development Leader for Lotus Sametime in IBM's Israel Software Laboratory (ILSL). She joined the Sametime group 12 years ago after spending 10 years as a Software Engineer in several companies. She has filled various development and development leadership roles within ILSL, in the Sametime group and in the SIP presence server group. You can reach her at GILIR@il.ibm.com.

Trademarks

- Domino, IBM, Lotus, Notes, Tivoli, Sametime, and WebSphere are trademarks or registered trademarks of IBM Corporation in the United States, other countries, or both.
- Microsoft and Windows are registered trademarks of Microsoft Corporation in the United States, other countries, or both.
- Java and all Java-based trademarks and logos are trademarks or registered trademarks of Sun Microsystems, Inc. in the United States, other countries, or both.
- Other company, product, and service names may be trademarks or service marks of others.