



La sicurezza secondo skymeeting

(data pubblicazione 06/12/2011)



La sicurezza nel sistema di videoconferenza Skymeeting

skymeeting è un sistema di videoconferenza web-based che utilizza la rete internet per collegare utenti geograficamente remoti tra loro. **skymeeting** considera la sicurezza una priorità assoluta nella progettazione della propria piattaforma e delle applicazioni ad essa collegate. Per questo motivo, **skymeeting** può essere integrato con piena affidabilità nelle procedure di business di aziende e organizzazioni che osservano politiche particolarmente restrittive in termini di sicurezza.

skymeeting garantisce elevati livelli di sicurezza, sia nell'erogazione dei contenuti audio e video che nella protezione delle informazioni utente, attraverso l'utilizzo di una serie di tecnologie allineate ai più alti standard adottati sul web.

Come in ogni sistema complesso, le caratteristiche di sicurezza non dipendono da una singola tecnologia, ma sono il risultato dell'interazione coordinata di diverse tecnologie applicate alle varie componenti che costituiscono l'infrastruttura: hardware, software, collegamenti, logiche, persone e così via.

Grazie alla puntuale progettazione di questa struttura, **skymeeting** assicura una risposta adeguata alle principali esigenze di sicurezza degli ambienti di videoconferenza:

- minimizzare i rischi derivanti da possibili minacce esterne ai sistemi hardware e software di videoconferenza, inclusi i sistemi client e le loro reti;
- prevenire l'utilizzo non autorizzato del servizio e delle sue funzionalità e garantire che solo il conduttore e i partecipanti dallo stesso autorizzati possano accedere ad una sessione online;
- assicurare la riservatezza dei dati utente e delle comunicazioni;
- mantenere elevati e costanti livelli di disponibilità del servizio, evitando malfunzionamenti o interruzioni;
- integrare il sistema di videoconferenza all'interno dei sistemi di business dell'utente, preservandone il livello di affidabilità e adeguandosi alle politiche di sicurezza già esistenti.

La sicurezza di **skymeeting** si articola in 5 macro aree, che globalmente disegnano una struttura robusta e affidabile in grado di garantire elevati livelli di disponibilità, riservatezza e protezione di ogni interazione degli utenti fra di loro e con il sistema.

Qui di seguito è descritta brevemente la struttura e le caratteristiche delle varie macro aree costituenti la sicurezza di **skymeeting**.

Sicurezza dell'infrastruttura

L'infrastruttura di **skymeeting** è costituita da potenti server in linea con i più recenti standard tecnologici e ospitati nei data center dei principali operatori italiani di hosting e telecomunicazioni. I data center offrono le migliori garanzie di protezione fisica e ambientale e attuano misure che assicurano la continuità elettrica, la connettività e il pronto intervento in caso di anomalie. Tutte le funzionalità di **skymeeting** sono ridondate, in modo che nessun guasto possa interrompere il servizio (nessun "single point of failure").

I server sono dotati di firewall e antivirus; la loro configurazione è improntata alla massima sicurezza compatibile con i servizi da erogare. Ad esempio, è prevista esclusivamente la sola attivazione delle porte TCP necessarie al funzionamento del sistema.

Gli accessi al back end dell'infrastruttura sono riservati esclusivamente allo staff IT di **skymeeting** e sono protetti da sistemi di autenticazione forte e monitoraggio costante.

Tutti i dati utente, le registrazioni dei meeting e le configurazioni vengono quotidianamente sottoposti a backup completi e incrementali.



Tutti i server sono di proprietà di **skymeeting**, così come pure il software applicativo. La manutenzione di tutto il sistema è effettuata da personale interno, debitamente formato e addestrato. Nessun dipendente o collaboratore di aziende terze ha accesso al sistema.

Sicurezza dei meeting

Le politiche di sicurezza dell'accesso ai meeting sono regolate tramite l'utilizzo di ruoli predefiniti. Attraverso l'interfaccia amministratore, è possibile modulare il livello di sicurezza dei meeting, controllando i privilegi di ogni persona autorizzata ad accedere ai meeting.

I ruoli previsti all'interno dell'ambiente **skymeeting** sono 4:

- **Amministratore**: può creare, rimuovere e configurare meeting room, organizzare meeting, caricare contenuti, invitare partecipanti, creare e rimuovere altri operatori ed assegnare loro un ruolo.
- **Operatore avanzato**: dispone di tutte le funzioni dell'amministratore, ad eccezione dell'aggiunta/rimozione di altri operatori.
- **Conduttore**: può esclusivamente condurre un meeting che gli è stato assegnato e modificare la propria password.
- **Partecipante**: può solo accedere ai meeting per i quali gli siano state fornite le credenziali di accesso.

La protezione della riservatezza di un meeting, ossia l'impossibilità da parte di utenti non invitati di accedere ad un meeting, viene assicurata dalle seguenti caratteristiche dell'ambiente di **skymeeting**:

- Possibilità di impostare una password per l'accesso al meeting: solo i partecipanti in possesso di password possono accedere.
- Tutti gli utenti (conduttore e partecipanti) hanno piena visibilità sull'elenco delle persone connesse al meeting. In ogni momento il conduttore può invitare un partecipante ad identificarsi attivandolo in audio e video, e se necessario può escluderlo dal meeting.
- I canali audio e video delle sessioni di videoconferenza transitano su internet in modalità crittografata (v. il punto 4 di seguito). Pertanto il contenuto dei meeting è disponibile esclusivamente ai partecipanti che hanno effettuato regolare accesso al sistema.
- Possibilità di programmare meeting riservati (meeting "privati"), con particolari restrizioni per l'accesso:
 - Partecipanti profilati: per partecipare ad un meeting privato un partecipante deve essere inserito nella lista utenti.
 - Accesso con autenticazione: l'accesso al meeting deve essere necessariamente effettuato tramite autenticazione del partecipante. Solo dopo l'autenticazione, il partecipante potrà accedere al meeting privato; nella propria area riservata visualizzerà solo i meeting a cui è stato invitato a partecipare.
 - Il sistema non provvede a recapitare via e-mail le credenziali di accesso all'area partecipante privata (anche se consente di farlo, a discrezione dell'amministratore). Per maggiore sicurezza, tali credenziali possono essere consegnate al partecipante tramite altri mezzi di comunicazione (personalmente, via SMS o per telefono).
 - Le informazioni relative ad un meeting (data, ora, argomento, conduttore) non compaiono nella pagina di accesso ai meeting e sono pertanto invisibili e non riconoscibili per chi non è invitato.

Sicurezza delle transazioni

Ogni comunicazione via internet è potenzialmente soggetta alla minaccia di hacker che, frapponendosi nelle interazioni fra i client e i server, tentano di intercettarne e ricostruirne il contenuto. Per questo



motivo, già da tempo, su internet esistono standard industriali di sicurezza largamente utilizzati laddove i contenuti che transitano sulla rete necessitano di protezione e riservatezza.

skymeeting utilizza e combina questi sistemi di protezione per ottenere un elevato livello di sicurezza in tutte le transazioni.

Quando un utente interagisce con l'ambiente di videoconferenza, il suo browser stabilisce un collegamento sicuro con i server di **skymeeting**. Tale collegamento è crittografato attraverso il protocollo SSL/TLS, lo standard tipicamente utilizzato nelle transazioni che richiedono totale riservatezza (home banking, acquisti con carte di credito e simili). In tal modo username, password, contenuti utente e ogni altra informazione che transita su internet attraverso il protocollo web sono protetti dal canale crittografico.

E' possibile verificare l'attivazione del protocollo crittografico controllando che nella barra degli indirizzi le URL siano precedute dalla sigla "https" e sia presente il simbolo "lucchetto" nell'interfaccia del browser (la posizione del lucchetto varia a seconda del browser: a sinistra della barra indirizzi per IE e Safari, a destra per Chrome e Opera, in basso a destra sulla barra di stato per Firefox).

skymeeting utilizza per la crittografia e per l'identificazione sicura dei propri server nei confronti del browser del cliente un certificato emesso da una Certification Authority internazionalmente riconosciuta (Comodo Group Inc.).

Sicurezza della tecnologia Flash

I servizi di videocomunicazione di **skymeeting** sono integralmente fruibili tramite browser internet e sono basati sulla tecnologia Flash. Si tratta una piattaforma che prevede - lato client - un runtime di dimensioni contenute (plugin), e che è ampiamente utilizzata per realizzare interfacce web arricchite da elementi multimediali. In ambienti business, la tecnologia Flash è usata per applicazioni di comunicazione di classe enterprise.

Flash supporta e integra numerosi protocolli di sicurezza e si integra con tutti i più diffusi meccanismi di autenticazione e di controllo degli accessi, rendendo disponibili ed efficaci i metodi di protezione già esistenti negli ambienti in cui viene impiegato.

Allo stesso tempo, il plugin Flash che gira sulle macchine client (Flash Player) ed è progettato per funzionare in modo isolato rispetto al resto dell'ambiente del computer (security sandbox), disponendo costantemente in tal modo di un accesso limitato e protetto alle risorse del sistema operativo: ad esempio, Flash Player non ha alcun accesso a file e dati presenti sui dischi locali o di rete o a informazioni contenute nella memoria. Anche se è prevista e consentita, da parte delle applicazioni Flash, l'archiviazione di informazioni sul computer locale, questo comportamento è revocabile in qualunque momento da parte dell'utente, attraverso apposite funzionalità di configurazione locale del plugin.

Più in generale, nelle organizzazioni che attuano una politica di sicurezza unificata, gli amministratori di rete possono definire centralmente i permessi di Flash Player relativi alla privacy e alla sicurezza (come la possibilità di memorizzare informazioni locali, l'accesso alle risorse multimediali e la notifica degli aggiornamenti).

Per questi motivi la tecnologia Flash è particolarmente resistente all'attacco di virus, trojan horse, backdoor worms e spyware. Inoltre, il Flash Player è un eseguibile binario e compilato, e come tale non è soggetto alle vulnerabilità dei linguaggi di scripting (tipicamente SQL injection e cross-scripting).

Infine, **skymeeting** utilizza una versione crittografata del protocollo Flash per la diffusione efficiente dei contenuti multimediali, garantendo che tutti i flussi audio e video scambiati fra i partecipanti ai meeting transitino sulla rete internet in forma protetta.



Sicurezza delle procedure

skymeeting progetta e realizza internamente tutto il software applicativo della piattaforma di videoconferenza. Sia l'architettura che il disegno dei flussi operativi sono stati realizzati con l'obiettivo di rispondere efficacemente ai più restrittivi requisiti di sicurezza informatica. Le caratteristiche progettuali del software di **skymeeting**, abbinate a procedure di lavoro standardizzate e ben conosciute da tutto lo staff, vanno a rafforzare la sicurezza intrinseca di tutto il sistema.

Citiamo, a titolo di esempio, alcune di queste caratteristiche:

- Tutte le password utente risiedono sui server in forma crittografata e non sono accessibili né conoscibili da parte dello staff interno. In caso di smarrimento, lo staff è in grado di resettare la password e recapitarne una nuova.
- I sistemi non prevedono forme di accesso automatiche: in tutti i casi in cui vengono utilizzati meccanismi di controllo remoto, gli utenti vengono informati da appositi messaggi e devono dare esplicito assenso. In qualsiasi momento un utente può revocare il controllo e uscire dalla sessione. Ogni collegamento è esplicitamente attivato o consentito da un utente (conduttore o partecipante) e non è previsto nessun meccanismo di collegamento automatico.
- I sistemi rispettano le misure di sicurezza delle reti utente: per il passaggio attraverso proxy e firewall vengono utilizzate le porte standard 80, 443 per la parte web, la porta 1935 per la parte audio/video e la porta 1936 per la funzionalità di Screen Sharing. Tutti i collegamenti ai sistemi sono avviati dagli utenti, ossia lato client e attraversano i firewall verso l'esterno. **skymeeting** non tenta alcuna connessione verso l'interno delle reti utente.



Schema a blocchi dell'infrastruttura skymeeting

Qui di seguito è possibile vedere la schematizzazione a blocchi dell'infrastruttura **skymeeting**:

