Cible de sécurité

Discretio entreprise

Révisions

Date	Version	Description	Auteur
03/10/2014	1.0	Création du document	MBDSYS
25/11/2014	1.1	Modification des composants et versions	MBDSYS
13/11/2015	1.2	Modifications suite au rapport d'évaluation	MBDSYS

Sommaire

1 Identification du produit

Organisation éditrice	MBDSYS
Lien vers l'organisation	https://www.discretio.com http://mbdsys.com/
Nom commercial du produit	Discretio entreprise
Numéro de la version évaluée	1.2.0
Catégorie de produit	Téléphonie sur IP sécurisée

2 Argumentaire (description) du produit

2.1Description générale du produit

Le principal objectif de *Discretio* est de fournir un service communication sécurisé entre deux terminaux mobiles, raccordés à une infrastructure fixe de gestion des appels. La communication est établie sur un canal de données d'un opérateur de téléphonie mobile (4G, 3G, EDGE…) ou un réseau Wi-Fi.

La solution permet d'authentifier les utilisateurs et de chiffrer les communications entre deux terminaux mobiles.

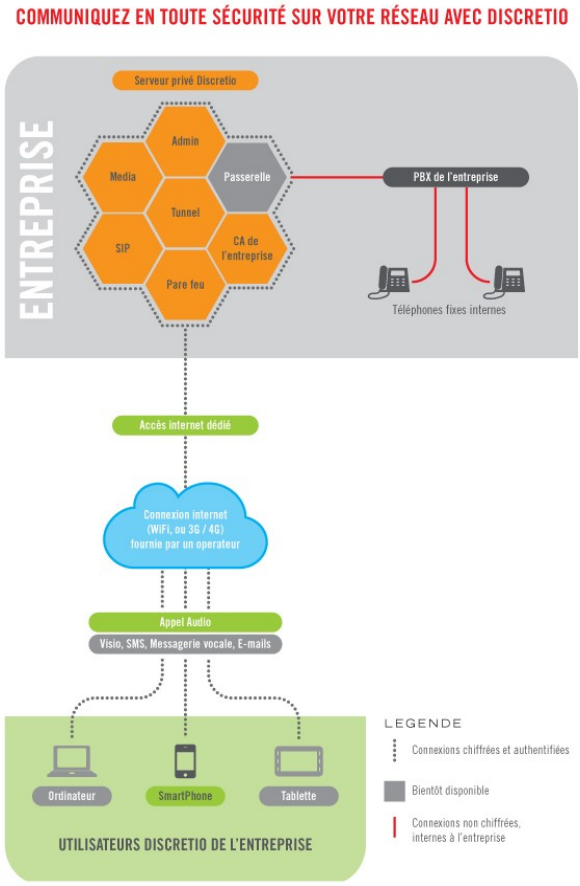

Figure : Schéma général

La solution est composée :

- d'une application « Discretio » tournant sur un terminal mobile Android ;

- d’un serveur de signalisation (Kamailio) pour l’établissement de la session entre les terminaux ;
- d’une infrastructure à clés publique composé d’une autorité de certification (AC) et d’une autorité d’enregistrement (AE) assurée par un service web.

Les fonctions de sécurité principales du produit sont :

- l’authentification mutuelle : chacun des terminaux possède une clé privée et un certificat utilisés pour s’authentifier auprès des serveurs et des autres utilisateurs ;
- la confidentialité des échanges entre le terminal et le serveur d’enregistrement : le terminal se connecte de façon sécurisée au serveur d’enregistrement, à l’aide du protocole HTTPS ;
- la confidentialité des échanges entre le terminal et le serveur de signalisation : le terminal se connecte de façon sécurisé au serveur de signalisation à l’aide du protocole SIP transportée de façon chiffrée grâce à un canal TLS ;
- la confidentialité des communications audio : les communications audio sont chiffrées grâce à un secret échangé à l’aide du protocole Diffie-Hellman (DH), au travers de la connexion au serveur de signalisation Kamailio;

L’ensemble de la solution est disponible en open-source.

2.2Description de l’utilisation du produit

Une fois l'application installée sur le terminal, le terminal s’enregistre auprès du système en générant en local une clé privée et une demande de signature de certificat (RSA2048, SHA256), qui est ensuite envoyé à un service web pour être signé après une procédure de vérification (consistant à envoyer à l’utilisateur un token qu’il réutilisera pour valider que le numéro de téléphone associé au certificat est légitime).

Un utilisateur souhaitant appeler de façon sécurisée doit être connecté à un réseau de données, et s’être enregistré auprès du service Discretio.

Lorsqu’un utilisateur souhaite passer un appel, l’application interagit avec le serveur de signalisation pour mettre en relation les deux utilisateurs, la communication passe ensuite par le biais du serveur proxy.

Un administrateur se connecte directement (en point à point) avec le serveur au travers d’une liaison Ethernet et administre le serveur en s’authentifiant au travers d’une interface web.

2.3 Description de l’environnement d’utilisation du produit

Discretio consiste en deux composants :

- Discretio client : application tournant sur un téléphone Android
- Serveur Privé Discretio : prévu pour fonctionner en tant qu’appliance matérielle, il est livré préinstallé, contenant l’ensemble des services utilisés par la solution (serveur de signalisation, proxy SIP, autorité de certification, pare-feu…).

2.3.1 Matériel compatible ou dédié

Les téléphones recommandés lors de la rédaction de ce document sont les modèles suivants :

- Samsung Galaxy S4

2.3.2 Environnement système

Les versions suivantes ont été retenues :

- Discretio client

  Android >= 5.0.1

- Serveur Privé Discretio

  Ubuntu Server 14.04 LTS

2.3.3 Environnement physique

Le composant Serveur Privé Discretio est connecté sur Internet d'une part, et connecté directement à un poste d'administration, en point-à-point, sans passer par le réseau local de l'entreprise.

Ce dernier est situé dans des locaux considérés comme sécurisés.

2.3.4 Versions

Les versions des différents composants de la solution sont les suivantes :

- Discretio (client) : 1.2.0
- Serveur Privé Discretio : 0.1.579
- Serveur SIP : kamailio 4.0.0-ssl127
- Couche réseau serveur sslisl : 0.1.861
- Couche réseau client sslisl : 0.1.860
- Composants externes au client
    - openssl 1.0.2d
- Composants externes serveur
    - Apache2 2.4.7
    - python-webpy 0.37
    - openssl 1.0.1f
    - openssl 1.0.2 beta 3

3 Biens sensibles que le produit doit protéger

Discretio permet de communiquer de façon sécurisée avec un ensemble d’utilisateurs identifiés et authentifiés auprès du système.

3.1Données utilisateurs

La clef privée de l’utilisateur est stockée sur le téléphone. Cette clef privée doit rester cohérente avec la clef publique associée. Elle est protégée par une clef (mot de passe) utilisée pour la déchiffrer. La clef privée et le mot de passe doivent rester confidentiels. Le certificat de l’utilisateur doit rester intègre.

Les communications entre deux utilisateurs doivent rester confidentielles.

4 Description des menaces

Un attaquant externe réussit à :

- déchiffrer les communications entre un terminal et un serveur, ou entre deux terminaux ;
- usurper l'identité d'un utilisateur, en obtenant un certificat possédant le même numéro de téléphone.;

Les hypothèses suivantes sont émises concernant l'environnement de la solution :

- les administrateurs sont considérés comme non hostiles. Ils sont formés pour les tâches qu'ils ont à effectuer et se conforment aux procédures et documentations existantes ;
- il n'y a pas d'applications malveillantes ayant un accès root installées sur le téléphone ;
- l'autorité de certification racine de la solution est considérée comme sûre;
- lorsque le téléphone n'est pas utilisé, ce dernier est verrouillé par un code ou un schéma de verrouillage
- l'utilisateur prévient l'administrateur dès qu'il s'aperçoit que son téléphone est perdu ou volé. L'administrateur révoque son certificat immédiatement.

5 Description des fonctions de sécurité du produit

5.1Chiffrement

La confidentialité entre le terminal et le serveur de signalisation (SIP) est assurée par :

- TLS 1.2 ;
- suite de chiffrement résultante : DHE-RSA-AES256-GCM-SHA384.
    - l'échange de clés Diffie-Hellman est utilisé avec un module d'une longueur de 2048 bits ;

La confidentialité entre le terminal et le service d'enregistrement (HTTP) est assurée par :

- TLS 1.2 ;
- suite de chiffrement : DHE-RSA-AES256-GCM-SHA384.
    - l'échange de clés Diffie-Hellman est utilisé avec un module d'une longueur de 2048 bits ;

La confidentialité des communications audio est assurée par :

- protocole SRTP (rfc 3550) :
    - suite de chiffrement AES-CM-128-HMAC-SHA1-80 ;
    - codec SPEEX-nb ;
- les clés utilisées par le protocole SRTP sont échangées par Diffie-Hellman avec un module d'une longueur de 2048 bits. Ces échanges sont signés à l'aide d'un HMAC-SHA2-256 (primitives EVP_DigestXXX de openssl) ;

5.2Authentification

L’authentification repose sur l’utilisation de certificats numériques :

- un utilisateur peut s’authentifier auprès des serveurs et des autres utilisateurs ;
- la chaîne de confiance est vérifiée à l’aide des trois certificats stockés dans le téléphone : celui l’AC racine, et des AC intermédiaires (l’une signant les certificats clients, l’autre les certificats des serveurs).

Les clients s’authentifient entre eux à l’aide de :

- la vérification de la chaîne de confiance ;
- la vérification du CommonName (numéro de l’appelant) ;
- des 16 premiers octets du champ "Subject Key Identifier" des certificats de l’appelé et d'appelant, affichés en hexadécimal sur les deux terminaux (Local xxxxx Peer xxxxx).

5.3Protection des clefs

La clef privée d’authentification de l’utilisateur est protégée en confidentialité. Cette dernière est conservée selon le standard PKCS8, encodée au format PEM et chiffrée à l’aide de l’algorithme AES256-CBC. La fonction de dérivation utilisée est PBKDF2 avec la fonction de hachage HMAC-SHA256, le nombre d’itération est 2048.

6 Spécifications des mécanismes cryptographiques

6.1Gestion des clés

Taille	La taille des clés publiques est de 2048 bits. L'exposant est 65537.
Mode de distribution	La clé publique d'un client sur un terminal mobile est distribuée par TCP/IP vers un serveur (service web). Les clés publiques des autorités de certifications sont intégrées dans le binaire de l'application du terminal mobile.
Procédé de génération	Les clés publiques et privées sont générées à l'aide des fonctions suivantes de la librairie OpenSSL : • mkreq() (dummyisl.cpp) ; • RSA_generate_key_ex() (openssl). Les clés pour les échanges DH sont générées à l'aide des fonctions suivantes : • DHProcessor::run() (dymmydh.cpp) ; • computeSessKey() (dummyisl.cpp) ; • DH_generate_key(), DH_compute_key() (openssl). L'application Android utilise de la librairie suivante : openssl 1.0.2d La partie serveur utilise la librairie suivante : openssl 1.0.1f, openssl 1.0.2 beta 3
Format de conservation	L'ensemble des clefs sont stockées au format PEM, et la clef privée est conservée selon le standard PKCS8 et chiffrée à l'aide de l'algorithme AES256-CBC.La fonction de dérivation utilisée est PBKDF2 avec la fonction de hachage HMAC-SHA256, le nombre d'itération est 2048.
Format de transmission	Les clés publiques (inclues dans les certificats X509) sont transmises : • sous format PEM lors de l'enregistrement ; • sous format DER encodé en base64 lors de l'initialisation d'une communication ; • suivant le standard TLS v1.2 lors de la connexion au serveur SIP.

6.2Traitement des données

Pré-traitements	Les données de signalisation respectent le standard SIP (rfc 3261), les en-têtes suivantes sont ajoutées en complément (pour l'appelant et pour l'appelé) : • X-CSL-Info1 et X-CSL-Info2 pour transmettre les données nécessaires à l'échange DH ; • X-CSL-From et X-CSL-From-Chain pour transmettre le certificat et le certificat de l'AC client de l'appelant. Les données des flux audio sont encodées avec le codec SPEEX-nb, et transmises selon le protocole RTP (rfc 3550). La communication avec le service d'enregistrement est effectuée en suivant le protocole HTTPS/TLS 1.2
Post-traitements	Les données de signalisation chiffrées suivent le protocole TLS 1.2 (rfc 5246), il n'y a pas de post-traitement en plus. Les données audio chiffrées suivent le protocole SRTP (rfc 3711), il n'ya pas de post-traitement en plus. Les données chiffrées transmises vers le service d'enregistrement respectent le protocole HTTPS/TLS 1.2.

7 Glossaire et références

AC	Autorité de certification
DER	Distinguished Encoding Rules : format d'encodage
OpenSSL	Suite d'outils et de librairies pour le chiffrement
PEM	Privacy Enhanced Mail
rfc 3261	SIP: Session Initiation Protocol (http://www.ietf.org/rfc/rfc3261.txt)
rfc 3550	RTP: A Transport Protocol for Real-Time Applications (http://www.ietf.org/rfc/rfc3550.txt)
rfc 5246	The Transport Layer Security (TLS) Protocol (Version 1.2) (http://www.ietf.org/rfc/rfc5246.txt)
SPEEX-NB	Codec de compression
TLS	Transport Layer Security
X509	Norme de cryptographie pour la gestion de certificats

Tableau Glossaire