

## Audit de réseaux VoIP

### 2 – Menaces

<b>Project phase</b>	WP6
<b>Author</b>	Juergen Ehrensberger, Alistair Doswald, Xavier Hahn, Sébastien Contreras
<b>Document creation</b>	18 octobre 2006
<b>Version</b>	1.0
<b>Latest modification</b>	18 octobre 2006
<b>Version control path</b>	

#### Résumé

*Ce document fait partie de la méthodologie d'audit de réseaux VoIP du projet Vadese. Il fournit les checklists pour la deuxième étape de l'audit, l'analyse des menaces. Elle permet de déterminer les menaces à considérer dans les phases suivantes et d'identifier les sources de menaces.*

© 2006 HES-SO

#### Relation avec les documents de l'audit VoIP

Ce document contient les checklists pour la deuxième étape de l'audit VoIP. La méthodologie d'audit générale est décrite dans le document « Audit sécurité VoIP » [1].

#### Structure du document

La première partie du document fournit les informations de base qui permettent de correctement effectuer l'audit. Ces informations sont relativement exhaustives et peuvent être consultées pour avoir de l'aide lors de l'audit.

La deuxième partie fournit les checklists qui permettent d'analyser les menaces.

# 1 Menaces et sources de menace

---

Une menace est le résultat d'une attaque ou d'une action involontaire ou négligente qui compromet la sécurité du réseau VoIP. Des sources de menaces potentielles sont donc des personnes malintentionnées ou les utilisateurs normaux. Les sources de menaces peuvent être internes ou externes au réseau VoIP.

## 1.1 Classification des menaces

---

Cette section décrit les différentes menaces auxquelles un réseau VoIP est exposé. Les services suivants sont considérés :

- service de base (appel simple),
- appels de conférence,
- boîte vocale,
- redirection d'appels.

Les services non considérés sont :

- messages vidéo
- messages instantanés,
- service de présence.

Catégorie	Sous-catégorie	Explication
<b>Déni de Service (DoS)</b>		
		Action volontaire ou involontaire entraînant l'indisponibilité d'un service/système pour les utilisateurs autorisés.
<b>Interruption de la communication en cours</b>		
		Action volontaire ou involontaire terminant une communication légitime ayant été établie précédemment.
<b>Empêcher l'établissement de la communication</b>		
		Action volontaire ou involontaire empêchant les utilisateurs légitime d'établir une communication vocale.
<b>Rendre la communication inaudible</b>		
		Action volontaire ou involontaire dégradant fortement la qualité d'une communication vocale.
<b>Epuisement de ressources</b>		
		Inondation de la cible avec des requêtes légitimes ou illégitimes, ce qui entraîne l'indisponibilité d'un service.
<b>Effacer des messages de la boîte vocale</b>		

		Action volontaire ou involontaire destinée à effacer les messages enregistrés sur la boîte vocale sans l'accord de l'utilisateur légitime de cette boîte vocale.
<b>Ecoute clandestine</b>		
		Action volontaire ou involontaire destinée à effacer les messages enregistrés sur la boîte vocale sans l'accord de l'utilisateur légitime de cette boîte vocale.
<b>Ecoute de la conversation</b>		
		Interception et reconstruction, enregistrement ou extraction du contenu de conversations téléphoniques.
<b>Ecoute non autorisée de messages de la boîte vocale</b>		
		Accès, reconstruction ou enregistrement de messages enregistrés sur une boîte vocale par un utilisateur non autorisé.
<b>Obtention d'informations sur le contenu de la communication</b>		
		Accès, reconstruction ou enregistrement de messages enregistrés sur une boîte vocale par un utilisateur non autorisé.
<b>Obtention d'informations sur les propriétés de la communication</b>		
		Interception du trafic de signalisation permettant d'obtenir des informations comme la durée de la communication, l'identité ou l'adresse IP des protagonistes.
<b>Détournement du trafic</b>		
		Reroutage de la signalisation ou du contenu d'une communication vers un autre système ou une autre personne sans l'accord des utilisateurs légitimes de la communication. Le détournement est dissimulé des utilisateurs légitimes.
<b>Détournement de l'appel</b>		
		Détournement du flux média d'un appel dans le but d'intercepter, enregistrer ou extraire le contenu.
<b>Détournement de la signalisation</b>		
		Détournement du trafic de signalisation dans le but d'extraire des informations sur le comportement des utilisateurs ou les caractéristiques des communications.
<b>Manipulation de l'identité et du contenu</b>		
		Modification du contenu des messages de signalisation ou du flux média, dans le but de tromper les autres utilisateurs.

	<b>Usurpation de l'identité</b>	
		Utilisation de l'identité d'un autre utilisateur dans le but de tromper le récepteur d'un message ou appel. Les utilisateurs sont principalement identifiés par leur « Caller-ID ».
	<b>Dissimulation de l'identité</b>	
		Dissimulation du Caller-ID dans le but de ne pas être reconnaissable par d'autres utilisateurs. La dissimulation peut être temporaire (établissement de l'appel) ou permanente (pendant toute la durée de l'appel).
	<b>Modification du contenu de communications</b>	
		Injecter des éléments dans une communication ou effacer des parties, dans le but modifier le contenu. Applicable à des appels ou des messages sur la boîte vocale.
<b>Vol de service</b>		
		Utilisation d'un service sans avoir à rémunérer son fournisseur ou sans avoir l'autorisation.
	<b>Tromper la taxation</b>	
		Empêcher la taxation correcte de l'utilisation d'un service, en manipulant l'identité ou en manipulant la taxation elle-même.
	<b>Utilisation non autorisée de services</b>	
		Utilisation d'un service par un utilisateur qui n'a pas d'autorisation pour ce service, en manipulant l'identité ou les droits de l'utilisateur.
<b>Communications non désirées</b>		
		Possibilité d'établir des communications que le destinataire aimerait filtrer. Bien que certains types de communications soient légaux, le destinataire doit avoir la possibilité d'empêcher des communications non désirées.
	<b>Appels SPAM</b>	
		Abus du service téléphonique pour l'établissement récurrent de communications non désirées.

## 1.2 Sources de menaces

Afin de pouvoir estimer le risque présenté par une menace, il est nécessaire d'analyser la source de la menace et ses motivations de réaliser une attaque.

La table suivante est basée sur [2].

Source de menace	Motivations	Actions typiques
Utilisateur interne mal formé ou négligent	Action involontaire ou négligente	<ul style="list-style-type: none"> <li>• Divulgence d'informations sensibles (mot de passe).</li> <li>• Violation de la politique de sécurité</li> </ul>
Utilisateur interne malintentionné, aussi ancien collaborateur	<ul style="list-style-type: none"> <li>• Curiosité</li> <li>• Bénéfice financier</li> <li>• Rancune</li> </ul>	<ul style="list-style-type: none"> <li>• Violation de la politique de sécurité, p.ex afin de simplifier le travail</li> <li>• Accès à des informations sensibles</li> <li>• Utilisation non autorisée de services</li> <li>• Sabotage du système</li> <li>• Chantage</li> </ul>
Administrateur mal formé ou négligent	Action involontaire ou négligente	<ul style="list-style-type: none"> <li>• Divulgence d'informations sensibles (mot de passe).</li> <li>• Violation de la politique de sécurité.</li> <li>• Configuration incorrecte d'un système</li> </ul>
Administrateur malintentionné, aussi ancien collaborateur	<ul style="list-style-type: none"> <li>• Curiosité</li> <li>• Bénéfice financier</li> <li>• Rancune</li> </ul>	<ul style="list-style-type: none"> <li>• Violation de la politique de sécurité, p.ex afin de simplifier le travail</li> <li>• Accès à des informations sensibles</li> <li>• Utilisation non autorisée de services</li> <li>• Sabotage du système</li> <li>• Chantage</li> </ul>
Hacker, cracker	<ul style="list-style-type: none"> <li>• Défi</li> <li>• Ego</li> </ul>	<ul style="list-style-type: none"> <li>• Intrusion dans le système</li> <li>• Utilisation non autorisée de services et de ressources</li> <li>• Déni de service simple</li> </ul>
Criminel informatique	<ul style="list-style-type: none"> <li>• Bénéfice financier</li> <li>• Vol d'informations</li> <li>• Utilisation non autorisée de ressources</li> </ul>	<ul style="list-style-type: none"> <li>• Intrusion dans le système</li> <li>• Utilisation non autorisée de services et de ressources</li> <li>• Déni de service sophistiqué</li> </ul>
Espionnage industriel (compétiteurs, criminels informatiques)	<ul style="list-style-type: none"> <li>• Avantage compétitif</li> <li>• Bénéfice financier</li> <li>• Nuire à la</li> </ul>	<ul style="list-style-type: none"> <li>• Vol d'informations</li> <li>• Accès à des informations sensibles</li> <li>• Social engineering</li> </ul>

	réputation	
--	------------	--

### 1.3 Niveau de protection requis

---

La politique de sécurité d'une entreprise doit trouver un compromis entre le niveau de sécurité à réaliser et le coût. Dans une première étape, l'entreprise doit décider quel niveau de protection est nécessaire pour chaque menace.

La table suivante définit les niveaux de protection qu'une entreprise peut exiger contre les différentes menaces.

Protection	Explication
<b>Elevé</b>	La menace doit être prévenue avec une fiabilité très élevée contre des sources d'attaques hautement motivées et compétentes.
<b>Moyen</b>	La menace doit être prévenue avec fiabilité contre les attaques les plus courantes. La réalisation de la menace est tolérée dans des circonstances rares.
<b>Faible</b>	Aucune protection explicite n'est requise. La menace est jugée tolérable par l'entreprise, tenant compte des sources de menace potentielles, de leur motivation et de leur compétence.

## 2 Références

---

- [1] Projet VaDeSe : « Audit de la sécurité de réseaux VoIP » ; Version 1.0 ; Octobre 2006 ; HES-SO.
- [2] Gary Stoneburner, Alice Goguen, and Alexis Feringa ; *"Risk Management Guide for Information Technology Systems"*; Recommendations of the National Institute of Standards and Technology; Special Publication 800-30; July 2002; <http://csrc.nist.gov/publications/nistpubs>.

## 2 - Menaces

Description de l'audit :

---

---

---

Auditeurs :

---

Date début de l'audit :

---

Date fin de l'audit :

---

## 1 Menaces, source de menace et protection

Ce checklist permet d'énumérer les menaces. Le niveau de protection requis est déterminé par la société, tenant compte de la politique de sécurité de la société.

### Légende

- **Menace** : nom des menaces à considérer. Voir ci-dessus.
- **Source de menace** : Utilisateur interne négligeant, utilisateur interne malintentionné, administrateur négligeant, administrateur malintentionné, hacker, criminel informatique, espionnage industriel.
- **Niveau de protection** : niveaux de protection qu'une entreprise peut exiger contre les différentes menaces : élevé, moyen, faible.

Menaces, sources de menace et niveau de protection		
Menace	Sources de menace	Niveau de protection requis
<b>Déni de Service</b>		
Interruption de la communication	Utilisateur interne négligeant	Elevé, moyen, faible
	Utilisateur interne malintentionné	
	Administrateur négligeant	
	Administrateur malintentionné	
	Hacker	
	Criminel informatique	
	Espionnage industriel	
Empêcher l'établissement de la communication		
Rendre la communication inaudible		
Epuisement des ressources		
Effacer des messages de la boîte vocale		
<b>Ecoute clandestine</b>		
Ecoute de la conversation		
Ecoute non autorisée de messages de la boîte vocale		
Obtention d'informations sur le contenu de la communication		
Obtention d'informations sur les propriétés de la communication		
<b>Détournement du trafic</b>		
Détournement d'un appel		
Détournement de la signalisation		
<b>Manipulation de l'identité et du contenu</b>		

Usurpation de l'identité		
Dissimulation de l'identité		
Modification du contenu de communications		
<b>Vol de service</b>		
Tromper la taxation		
Utilisation non autorisée de services		
<b>Communications non autorisées</b>		
Appels SPAM		

**Remarques**