



Ceci est un extrait électronique d'une publication de
Diamond Editions :

<http://www.ed-diamond.com>

Retrouvez sur le site tous les anciens numéros en vente par
correspondance ainsi que les tarifs d'abonnement.

Pour vous tenir au courant de l'actualité du magazine, visitez :

<http://www.gnulinuxmag.com>

Ainsi que :

<http://www.linux-pratique.com>

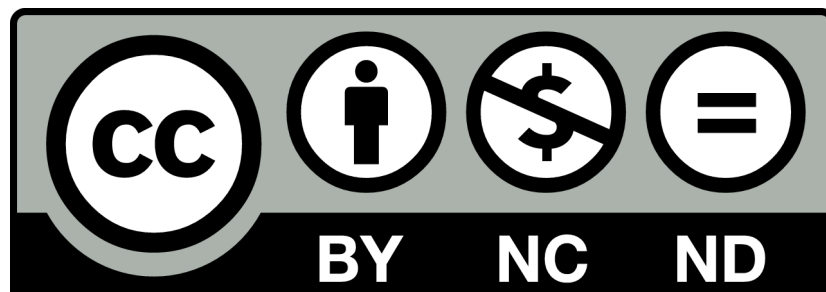
et

<http://www.miscmag.com>



Ceci est un extrait électronique d'une publication de Diamond Editions

<http://www.ed-diamond.com>



Creative Commons

Paternité - Pas d'Utilisation Commerciale - Pas de Modification 2.0 France

Vous êtes libres :

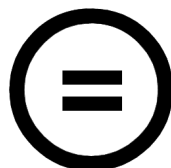
- de reproduire, distribuer et communiquer cette création au public.



Paternité. Vous devez citer le nom de l'auteur original de la manière indiquée par l'auteur de l'oeuvre ou le titulaire des droits qui vous confère cette autorisation (mais pas d'une manière qui suggérerait qu'ils vous soutiennent ou approuvent votre utilisation de l'oeuvre).



Pas d'Utilisation Commerciale. Vous n'avez pas le droit d'utiliser cette création à des fins commerciales.



Pas de Modification. Vous n'avez pas le droit de modifier, de transformer ou d'adapter cette création.

A chaque réutilisation ou distribution de cette création, vous devez faire apparaître clairement au public les conditions contractuelles de sa mise à disposition.

- Chacune de ces conditions peut être levée si vous obtenez l'autorisation du titulaire des droits.
- Rien dans ce contrat ne diminue ou ne restreint le droit moral de l'auteur ou des auteurs.

Ceci est le Résumé Explicatif du Code Juridique. La version intégrale du contrat est attachée en fin de document et disponible sur :

<http://creativecommons.org/licenses/by-nc-nd/2.0/fr/legalcode>

→ Netfilter Workshop 2005, conférence utilisateurs et développeurs

Éric Leblond

EN DEUX MOTS Le quatrième atelier de travail de Netfilter, NFWS2005, a eu lieu à Séville du 3 octobre au 8 octobre 2005. Cet événement rassemble chaque année la plupart des développeurs de la couche pare-feu de Linux afin qu'ils puissent discuter des évolutions à venir. Pour la première fois lors de cette édition, une conférence utilisateurs (comprendre administrateurs système) a eu lieu lors des 2 premiers jours.

Astaro, Mara Systems, Balabit ou encore INL qui emploient ou financent à elles seules une bonne partie des développeurs de Netfilter.

Ces fonds ont permis, d'une part, de distribuer des *goodies* très appréciés comme des T-shirts ou des pochettes et, d'autre part, de prendre en charge les frais de déplacement dans Séville et les repas de l'ensemble des participants de l'atelier des développeurs.



Unix pour le pare feu, le bon choix en Espagne et ailleurs (Photo réalisée sans trucage)

(3-4 octobre) Conférence utilisateur Une organisation impeccable

Le quatrième atelier de travail Netfilter s'est déroulé dans les locaux de l'Escuela Técnica Superior De Ingeniera Informatica de l'université de Séville. L'accueil sur place a été très chaleureux. L'organisateur Pablo Neira a en effet réuni une équipe de plusieurs personnes chargées de régler les problèmes pratiques.

Il a de plus réussi à rassembler des fonds en faisant appel au sponsoring, d'une part, d'entités régionales de promotion du Logiciel libre et, d'autre part, d'entreprises comme



Rusty Russell, auteur de *ipchains* et auteur original de Netfilter, et Harald Welte, chef actuel de l'équipe de Netfilter (de gauche à droite)



Pablo Neira, développeur de l'outil *conntrack* et organisateur de NFWS2005, dans le hall de l'hôtel

Ce dernier point a été très important puisqu'il a renforcé la convivialité des repas et de la manifestation en général en évitant les additions compliquées et en mettant tous les participants sur un pied d'égalité (financière). Si l'on ajoute à cela le côté *open source* des tapas où le partage est de mise, on comprend alors parfaitement la bonne ambiance régnant lors des moments de détente.

La manifestation se déroulant sur plusieurs jours, et les participants venant d'un peu partout dans le monde, la question du logement était cruciale. Une partie d'un hôtel a donc été réservée pour loger les développeurs, ce qui a indéniablement apporté beaucoup au niveau du règlement des déplacements et de la convivialité.

Des exposés variés

Après l'ouverture de la conférence par des autorités politiques locales, nous avons assisté à une suite de conférences techniques.

La plupart d'entre elles étaient d'un niveau élevé ; les développeurs ou tout au moins des contributeurs étant aux commandes, les explications étaient pour le moins complètes.

Du fait de la complexité des sujets abordés, je ne ferai ici qu'un compte-rendu partiel des exposés me concentrant sur ceux m'étant apparus comme les plus significatifs.



NOTE

Le classement engage l'auteur qui s'est efforcé d'être le plus impartial possible.

Présentation de l'outil contrack

Depuis très longtemps, une des plus fortes demandes des utilisateurs de Netfilter est l'ajout d'une interaction avec le système de suivi de connexions. Les requêtes les plus fréquentes concernent la modification depuis l'espace utilisateur d'entrées de la table de connexions ou encore une infrastructure cohérente de consultation du contrack.

Cela est maintenant possible, grâce à la bibliothèque `libcontrack` et à l'outil `contrack` présentés à la conférence par leur développeur Pablo Neira.

La commande `contrack` permet d'ajouter, modifier ou encore supprimer des entrées de la table de connexions. Une deuxième option permet tout simplement d'afficher la liste des connexions.

Bien que semblant triviale, cette fonctionnalité permet de régler un problème de conception : l'utilisation du pseudo-fichier `"/proc/net/ip_contrack"` employé jusqu'ici à cet effet avait en effet tendance à bloquer la machine lors de sa consultation.

Enfin, un mode passif permet de recevoir en espace utilisateur les événements issus du système de suivi de connexions. Cet outil s'appuie sur des nouvelles fonctionnalités qui ont été incorporées au noyau 2.6.14.

ipset et les spammers

Cet exposé de Jozsef Kadlecik a été le point d'orgue de la première journée, occupant une bonne partie des conversations lors du repas du soir.

Il a en effet présenté `ipset` qui est un système permettant de gérer des listes d'objets et de les utiliser comme correspondance dans des règles `iptables`. Les classes d'objets supportés sont variées (machine, réseau, ports) et les performances lors

des recherches de correspondance sont excellentes.

Il est donc possible de construire des jeux de règles complets mais factorisés et beaucoup plus rapides grâce à `ipset`. De plus, `ipset` permet aussi de réaliser des configurations intéressantes, comme illustré dans l'exemple suivant.

```
ipset -N spammers iptree --timeout $((60*60*24*7))
iptables -A FORWARD -d HONEYPOT -p tcp --dport 25 -j SET --add-set spammers src
iptables -A FORWARD -p tcp --dport 25 -m set --set spammers -j TARPIT
```

La première ligne définit un ensemble appelé « spammers ». Toute machine ajoutée à cette ensemble y reste une semaine (le paramètre `timeout` est précisé en secondes). La deuxième permet de peupler l'ensemble « spammers ».

La machine `HONEYPOT` est en fait une adresse IP qui n'est MX pour aucun domaine. Toute machine se connectant au port 25 du serveur est donc vraisemblablement animée d'intentions peu louables et voit donc son adresse IP ajoutée à l'ensemble « spammers ».

La troisième ligne enfin permet de ralentir (comprendre 10 min par mail) les machines de l'ensemble « spammers » lorsqu'elles tentent d'envoyer un mail vers les serveurs mail hébergés derrière le pare-feu.

`ipset` est donc un outil extrêmement intéressant qui permet de plus d'accroître considérablement les performances de Netfilter au prix toutefois d'un accroissement de la complexité de génération des règles.

L'espace utilisateur pour les développeurs noyau

L'exposé de Rusty Russell, ou plutôt le show à l'américaine de l'australien, a été un des grands moments de détente de la conférence.

Il avait ramené d'Australie des *Caramello Koala* afin de les lancer à ceux qui, dans la foule, répondaient correctement aux questions qu'il posait.

Pour ce qui était du contenu de l'exposé, il était également assez original puisqu'il s'agissait de proposer aux développeurs noyau un retour vers le développement en espace utilisateur.

Dans cette optique, une bonne partie de la conférence a été occupée à la présentation de

nsfsm, Netfilter Simulator, qui permet de tester en espace utilisateur les développements de module Netfilter.

Cet outil permet de compiler un binaire contenant les fonctions Netfilter du noyau à tester. D'un point de vue utilisation, il se présente comme une interface en ligne de commandes acceptant les instructions de routages, les commandes iptables et des commandes dédiées.

La commande `gen_ip`, par exemple, envoie des paquets IP et vérifie ensuite chaque étape de leurs parcours dans cette simulation de noyau.

Une fonctionnalité intéressante est offerte par la fonction `expect` qui permet de spécifier le résultat attendu (sortie par `eth1` par exemple). Il est ainsi possible de construire des scripts complexes pour vérifier l'état des fonctionnalités présentes dans un noyau.

NuFW, Now User Filtering Works

Dans cette conférence, j'ai présenté le projet NuFW partant des motivations du filtrage utilisateurs qui est le but principal du projet. J'ai insisté sur l'apport de l'authentification a posteriori par rapport aux autres solutions et j'ai continué sur les fonctionnalités avancées comme le routage par utilisateur et l'authentification unique.

L'exposé s'est terminé par une description des évolutions possibles grâce aux récents travaux sur le conntrack.



NOTE

L'auteur ne souhaitant pas ici faire sa publicité, nous vous proposons d'aller sur le site du projet pour une présentation plus détaillée des apports de NuFW.

NF hipac

La présentation de Michael Bellion a permis de faire la lumière sur son projet NF Hipac. Il s'agit d'un système permettant de classer extrêmement rapidement un paquet par rapport à un ensemble de règles ; bref, de savoir quelle est la règle qui s'applique à un paquet donné.

La figure 1 montre l'évolution du pourcentage de bande passante atteint lorsque l'on émet un maximum de paquets aléatoires d'une taille de 128 bytes sur un lien et que l'on augmente le nombre de règles de filtrage dans le système. Les performances du classificateur de Netfilter s'écroulent

alors que celles de NF hipac restent correctes. Il est bon de noter que le cas des paquets de 128 bytes est un cas pire (le nombre de paquet à traiter pour une bande passante donnée est inversement proportionnel à la taille des paquets). Pour des paquets plus gros, la bande passante de NF Hipac reste constante alors que celle de Netfilter s'écroule au bout d'un certain nombre de règles.

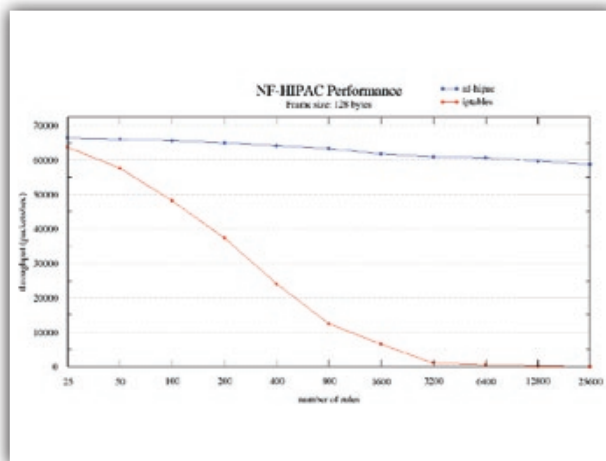


Fig. 1 : pourcentage de bande passante atteint suivant le nombre de règles

Les modifications du point de vue de l'administrateur sont de plus quasi inexistantes, car NF Hipac utilise comme entrée un jeu de règles similaire à celui de iptables.

C'est seulement ensuite qu'une optimisation très puissante est réalisée. L'idée de base est de ramener le problème itératif du test successif des règles à une suite de calcul de position d'un point par rapport à un ensemble d'intervalles.

Comme ce dernier problème est extrêmement rapide à résoudre et que le nombre de calculs de ce type nécessaire à la détermination complète du point est très faible (souvent 2 ou 3), la rapidité globale du classificateur NF Hipac est très largement supérieure à celle du classificateur natif de Netfilter, au prix d'une consommation mémoire plus élevée.

Bilan de la conférence utilisateurs

La conférence utilisateurs s'est terminée par le discours de Harald Welte sur les violations de la GPL. Ces deux jours ont donc été consacrés à des présentations abordables des travaux réalisés par la communauté du filtrage sur GNU/Linux ainsi qu'aux perspectives liées aux nouveaux projets qui ont ravis les participants.

(5-6 octobre) Conférence développeurs Un rythme effréné

La conférence développeur a commencé le troisième jour sur un tout autre ton. N'ayant que 2 jours (plus 2 jours de code) par an pour se dire les choses en face, l'équipe des développeurs de Netfilter dirigée par Harald Welte entame une liste d'exposés et de comptes-rendus sur un rythme



Derrière : Krisztian Kovacs (hu), Samir Bellabes (fr), Martin Josefsson (se), Alan Yang (us), Patrick McHardy (de), Pablo Neira (es), Henrik Nordstrom (se), Michael Bellion (de), Holger Eitzenberger (de), Balazs Scheidler (hu)
Devant : Jesse Peng (tw), Yasuyuki Kozakai (jp), Harald Welte (de), Rusty Russell (au), Jozsef Kadlecik (hu), Christian Hentschel (ar), Gert Hansen (de)

Derrière l'objectif : Éric Leblond

soutenu. Même la pause sieste a été sautée, les travaux reprenant directement après le repas du midi.

Premier jour « hashtrie » et la gestion du conntrack

Martin Josefsson a présenté ses travaux sur une nouvelle structure de données dédiée au stockage des informations liées au suivi de connexion.

Les performances de cette nouvelle structure sont excellentes en recherche puisqu'elles dépassent largement le système actuel. Elle n'en reste pas moins perfectible en suppression et insertion et Martin continue de travailler sur ce point.

Le constat ayant permis d'envisager cette structure est le fait qu'actuellement les processeurs sont beaucoup plus rapides que les accès mémoire. Une structure entraînant donc plus de calculs mais moins d'accès mémoire est donc potentiellement plus efficace qu'une structure (comme les tables de hash) qui nécessite plus d'accès mémoire que de calculs.

nfnetlink

L'utilisation de nfnetlink comme système de base et de référence pour les futurs développements est la décision marquante de la journée. Déjà intégrée au 2.6.14, NFnetlink est une infrastructure permettant des communications *Noyau* <-> *espace utilisateur* facilitées. Elle est basée sur netlink qui est le système de communication entre espace utilisateur et noyau déjà utilisé par le routage et les interfaces TAP. Le système netlink comporte 16 canaux dont bon nombre sont déjà alloués, l'utilisation de nombreux nouveaux canaux était donc impossible. NFnetlink permet donc de multiplexer un canal netlink qui devient alors dédié à Netfilter. De plus, un protocole d'échange de messages basique est prédéfini (UPDATE, NEW, DESTROY) et il est combiné à un système de messages encapsulés qui permet de supporter la plupart des évolutions. Cette évolutivité a permis d'utiliser ce système pour gérer la quasi-totalité des interactions entre espace utilisateur et noyau.

libnfnetlink_log

L'infrastructure de journalisation a été entièrement réécrite. Elle a permis le développement de Ulogd2 qui devrait bientôt voir le jour.

libnfnetlink_queue

Il s'agit, comme son nom l'indique, du successeur d'*ip_queue*. Cette fonctionnalité permet de prendre la décision pour un paquet donné ou d'en modifier le contenu en espace utilisateur.



câbles (tw), Balazs Scheidler (hu), Krisztian Kovacs (hu), Yasuyuki Kozakai (jp), Henrik Nordström (se), Harald Welte (de), Rusty Russell (au). (du premier au dernier plan)

Elle est utilisée par des projets comme snort-inline ou encore NuFW. `ip_queue` avait quelques défauts dont notamment l'absence dans le noyau officiel de la possibilité de marquer les paquets.

Les limitations inhérentes à `ip_queue` ont toutes volé en éclat.

► La limitation sur le nombre de queues disponible en parallèle passe de 1 à 65535.

► Le marquage des paquets est maintenant disponible d'origine.

libnfnetlink_conntrack et {lib}conntrack

Principalement développés par Pablo Neira et Harald Welte, ces bibliothèques et cet outil (décrits précédemment) sont d'une grande utilité et reposent totalement sur la nouvelle infrastructure nfnetlink.

Le noyau 2.6.14 comportera donc un nombre d'améliorations notables au niveau de la gestion des interactions entre Netfilter et l'espace utilisateurs.

Deuxième jour **Présentation de ipset**

Jozsef Kadlecsik a réalisé une présentation d'ipset et ippool plus technique que celle réalisée durant la conférence utilisateur et il a été convenu que l'incorporation dans la branche principale pourrait être envisagée après le port des modules et des outils de configuration vers nfnetlink.

L'inclusion de NF Hipac

Ce dernier jour a été marqué par le vote par la Core Team sur l'incorporation de NF Hipac au sein du noyau de Netfilter. Celle-ci a fait l'unanimité tant les performances obtenues grâce à NF Hipac dépassent celle de l'architecture actuelle.

La décision d'incorporer NF Hipac s'est aussi faite autour de points plus techniques. L'un des problèmes d'iptables est qu'il supporte mal l'ajout de règles. En effet, pour chaque modification, c'est l'ensemble de la table qui est envoyé au noyau. Ainsi pour un jeu de plusieurs milliers de règles, il faut recalculer l'ensemble de la table lorsque l'on ajoute une simple règle.

Cela explique notamment pourquoi le temps d'exécution d'un script est énormément plus long que le temps d'exécution d'iptables-restore. NF Hipac quant à lui utilise un système de messages envoyés grâce au système netlink pour mettre



La « Netfilter Core Team » : Jozsef Kadlecsik, Martin Josefsson, Harald Welte, Rusty Russell, Patrick McHardy



Au travail : Jozsef Kadlecik, Éric Leblond, Pablo Neira

à jour le jeu de règles, les modifications sont donc unitaires et c'est le kernel qui s'occupe d'appliquer le changement au jeu de règles. Cette incorporation avait été le sujet principal des discussions lors du précédent dîner. Les besoins plus importants en mémoire de NF Hipac constituaient la principale problématique, qui semble en effet incompatible avec son utilisation sur les systèmes embarqués.

NF Hipac utilise en effet un jeu linéaire de règles (comme iptables) et un système optimisé qui occupe une mémoire importante. La décision avait été officiellement prise la veille lorsque le problème de l'occupation mémoire avait été résolu en évoquant la possibilité d'utiliser uniquement le jeu linéaire de règles sur des installations nécessitant une empreinte mémoire réduite. Cette incorporation ne se fera pas sans difficultés ni travail. Il manque encore un certain nombre de fonctionnalités pour que les capacités de *matching* de NF Hipac soient équivalentes à celles de iptables.

Pour Michael Bellion, la compatibilité devrait actuellement être assurée pour environ 90% des installations. Il reste donc à assurer la compatibilité des 10 % d'installations restantes.



NFWS2005 est fini, mais il reste encore des Caramello Koala de Rusty Russell

(7-8 octobre) Coding days

Les *Coding days* ont clôturé l'atelier. Les développeurs, regroupés par sujet dans des petites entités, se sont penchés sur leur écran pour travailler toute la journée.

Le groupe spécialement dédié à l'incorporation de NF Hipac dans le noyau officiel a été l'un des plus actifs même si d'autres groupes comme celui s'occupant des bibliothèques utilisateurs pour le *conntrack* n'ont pas chômé.

Le dernier jour a été plus informel. L'université étant fermée le samedi et certains devant partir tôt pour prendre leur avion, seules quelques personnes se sont rassemblées dans des chambres de l'hôtel pour travailler. Les autres ont pour la plupart profité de la journée pour récupérer de la dernière soirée qui s'était terminée très tard.

Conclusion

NFWS2005 s'est donc terminé après une semaine aussi éprouvante que captivante. Les évolutions à venir de Netfilter sont enthousiasmantes tant d'un point de vue des fonctionnalités (*nfnetlink*, *ipset*) que d'un point de vue des performances avec l'arrivée probable de NF Hipac dans 2.6.16.

L'année 2005-2006 s'annonce comme un grand cru au niveau du filtrage sous GNU/Linux.



LIENS

Netfilter :

<http://www.netfilter.org/>

NFWS 2005 :

<http://workshop.netfilter.org/>

Téléchargement des présentations et programme :

<http://workshop.netfilter.org/users.html>

ipset :

<http://ipset.netfilter.org/install.html>

nfsim :

<http://ozlabs.org/~jk/projects/nfsim/>

NuFW : <http://www.nufw.org/>

NF Hipac : <http://www.hipac.org/>

Blog de la conférence : <http://nfws.inl.fr/>

Éric Leblond,

Creative Commons

Paternité - Pas d'Utilisation Commerciale - Pas de Modification 2.0

Creative Commons n'est pas un cabinet d'avocats et ne fournit pas de services de conseil juridique. La distribution de la présente version de ce contrat ne crée aucune relation juridique entre les parties au contrat présenté ci-après et Creative Commons. Creative Commons fournit cette offre de contrat-type en l'état, à seule fin d'information. Creative Commons ne saurait être tenu responsable des éventuels préjudices résultant du contenu ou de l'utilisation de ce contrat.

Contrat

L'Oeuvre (telle que définie ci-dessous) est mise à disposition selon les termes du présent contrat appelé Contrat Public Creative Commons (dénommé ici « CPCC » ou « Contrat »). L'Oeuvre est protégée par le droit de la propriété littéraire et artistique (droit d'auteur, droits voisins, droits des producteurs de bases de données) ou toute autre loi applicable. Toute utilisation de l'Oeuvre autrement qu'explicitement autorisée selon ce Contrat ou le droit applicable est interdite.

L'exercice sur l'Oeuvre de tout droit proposé par le présent contrat vaut acceptation de celui-ci. Selon les termes et les obligations du présent contrat, la partie Offrante propose à la partie Acceptante l'exercice de certains droits présentés ci-après, et l'Acceptant en approuve les termes et conditions d'utilisation.

1. Définitions

- a. « **Oeuvre** » : oeuvre de l'esprit protégeable par le droit de la propriété littéraire et artistique ou toute loi applicable et qui est mise à disposition selon les termes du présent Contrat.
- b. « **Oeuvre dite Collective** » : une oeuvre dans laquelle l'oeuvre, dans sa forme intégrale et non modifiée, est assemblée en un ensemble collectif avec d'autres contributions qui constituent en elles-mêmes des oeuvres séparées et indépendantes. Constituent notamment des Oeuvres dites Collectives les publications périodiques, les anthologies ou les encyclopédies. Aux termes de la présente autorisation, une oeuvre qui constitue une Oeuvre dite Collective ne sera pas considérée comme une Oeuvre dite Dérivée (telle que définie ci-après).
- c. « **Oeuvre dite Dérivée** » : une oeuvre créée soit à partir de l'Oeuvre seule, soit à partir de l'Oeuvre et d'autres oeuvres préexistantes. Constituent notamment des Oeuvres dites Dérivées les traductions, les arrangements musicaux, les adaptations théâtrales, littéraires ou cinématographiques, les enregistrements sonores, les reproductions par un art ou un procédé quelconque, les résumés, ou toute autre forme sous laquelle l'Oeuvre puisse être remaniée, modifiée, transformée ou adaptée, à l'exception d'une oeuvre qui constitue une Oeuvre dite Collective. Une Oeuvre dite Collective ne sera pas considérée comme une Oeuvre dite Dérivée aux termes du présent Contrat. Dans le cas où l'Oeuvre serait une composition musicale ou un enregistrement sonore, la synchronisation de l'oeuvre avec une image animée sera considérée comme une Oeuvre dite Dérivée pour les propos de ce Contrat.
- d. « **Auteur original** » : la ou les personnes physiques qui ont créé l'Oeuvre.
- e. « **Offrant** » : la ou les personne(s) physique(s) ou morale(s) qui proposent la mise à disposition de l'Oeuvre selon les termes du présent Contrat.
- f. « **Acceptant** » : la personne physique ou morale qui accepte le présent contrat et exerce des droits sans en avoir violé les termes au préalable ou qui a reçu l'autorisation expresse de l'Offrant d'exercer des droits dans le cadre du présent contrat malgré une précédente violation de ce contrat.

2. Exceptions aux droits exclusifs. Aucune disposition de ce contrat n'a pour intention de réduire, limiter ou restreindre les prérogatives issues des exceptions aux droits, de l'épuisement des droits ou d'autres limitations aux droits exclusifs des ayants droit selon le droit de la propriété littéraire et artistique ou les autres lois applicables.

3. Autorisation. Soumis aux termes et conditions définis dans cette autorisation, et ceci pendant toute la durée de protection de l'Oeuvre par le droit de la propriété littéraire et artistique ou le droit applicable, l'Offrant accorde à l'Acceptant l'autorisation mondiale d'exercer à titre gratuit et non exclusif les droits suivants :

- a. reproduire l'Oeuvre, incorporer l'Oeuvre dans une ou plusieurs Oeuvres dites Collectives et reproduire l'Oeuvre telle qu'incorporée dans lesdites Oeuvres dites Collectives;
- b. distribuer des exemplaires ou enregistrements, présenter, représenter ou communiquer l'Oeuvre au public par tout procédé technique, y compris incorporée dans des Oeuvres Collectives;
- c. lorsque l'Oeuvre est une base de données, extraire et réutiliser des parties substantielles de l'Oeuvre.

Les droits mentionnés ci-dessus peuvent être exercés sur tous les supports, médias, procédés techniques et formats. Les droits ci-dessus incluent le droit d'effectuer les modifications nécessaires techniquement à l'exercice des droits dans d'autres formats et procédés techniques. L'exercice de tous les droits qui ne sont pas expressément autorisés par l'Offrant ou dont il n'aurait pas la gestion demeure réservé, notamment les mécanismes de gestion collective obligatoire applicables décrits à l'article 4(d).

4. Restrictions. L'autorisation accordée par l'article 3 est expressément assujettie et limitée par le respect des restrictions suivantes :

- a. L'Acceptant peut reproduire, distribuer, représenter ou communiquer au public l'Oeuvre y compris par voie numérique uniquement selon les termes de ce Contrat. L'Acceptant doit inclure une copie ou l'adresse Internet (Identifiant Uniforme de Ressource) du présent Contrat à toute reproduction ou enregistrement de l'Oeuvre que l'Acceptant distribue, représente ou communique au public y compris par voie numérique. L'Acceptant ne peut pas offrir ou imposer de conditions d'utilisation de l'Oeuvre qui altèrent ou restreignent les termes du présent Contrat ou l'exercice des droits qui y sont accordés au bénéficiaire. L'Acceptant ne peut pas céder de droits sur l'Oeuvre. L'Acceptant doit conserver intactes toutes les informations qui renvoient à ce Contrat et à l'exonération de responsabilité. L'Acceptant ne peut pas reproduire, distribuer, représenter ou communiquer au public l'Oeuvre, y compris par voie numérique, en utilisant une mesure technique de contrôle d'accès ou de contrôle d'utilisation qui serait contradictoire avec les termes de cet Accord contractuel. Les mentions ci-dessus s'appliquent à l'Oeuvre telle qu'incorporée dans une Oeuvre dite Collective, mais, en dehors de l'Oeuvre en elle-même, ne soumettent pas l'Oeuvre dite Collective, aux termes du présent Contrat. Si l'Acceptant crée une Oeuvre dite Collective, à la demande de tout Offrant, il devra, dans la mesure du possible, retirer de l'Oeuvre dite Collective toute référence au dit Offrant, comme demandé. Si l'Acceptant crée une Oeuvre dite Collective, à la demande de tout Auteur, il devra, dans la mesure du possible, retirer de l'Oeuvre dite Collective toute référence au dit Auteur, comme demandé.

- b. L'Acceptant ne peut exercer aucun des droits conférés par l'article 3 avec l'intention ou l'objectif d'obtenir un profit commercial ou une compensation financière personnelle. L'échange de l'Oeuvre avec d'autres Oeuvres protégées par le droit de la propriété littéraire et artistique par le partage électronique de fichiers, ou par tout autre moyen, n'est pas considéré comme un échange avec l'intention ou l'objectif d'un profit commercial ou d'une compensation financière personnelle, dans la mesure où aucun paiement ou compensation financière n'intervient en relation avec l'échange d'Oeuvres protégées.
- c. Si l'Acceptant reproduit, distribue, représente ou communique l'Oeuvre au public, y compris par voie numérique, il doit conserver intactes toutes les informations sur le régime des droits et en attribuer la paternité à l'Auteur Original, de manière raisonnable au regard du médium ou au moyen utilisé. Il doit communiquer le nom de l'Auteur Original ou son éventuel pseudonyme s'il est indiqué ; le titre de l'Oeuvre Originale s'il est indiqué ; dans la mesure du possible, l'adresse Internet ou l'Identifiant Uniforme de Ressource (URI), s'il existe, spécifié par l'Offrant comme associé à l'Oeuvre, à moins que cette adresse ne renvoie pas aux informations légales (paternité et conditions d'utilisation de l'Oeuvre). Ces obligations d'attribution de paternité doivent être exécutées de manière raisonnable. Cependant, dans le cas d'une Oeuvre dite Collective, ces informations doivent, au minimum, apparaître à la place et de manière aussi visible que celles à laquelle apparaissent les informations de même nature.
- d. Dans le cas où une utilisation de l'Oeuvre serait soumise à un régime légal de gestion collective obligatoire, l'Offrant se réserve le droit exclusif de collecter ces redevances par l'intermédiaire de la société de perception et de répartition des droits compétente. Sont notamment concernés la radiodiffusion et la communication dans un lieu public de phonogrammes publiés à des fins de commerce, certains cas de retransmission par câble et satellite, la copie privée d'Oeuvres fixées sur phonogrammes ou vidéogrammes, la reproduction par reprographie.

5. Garantie et exonération de responsabilité

- a. En mettant l'Oeuvre à la disposition du public selon les termes de ce Contrat, l'Offrant déclare de bonne foi qu'à sa connaissance et dans les limites d'une enquête raisonnable :
 - i. L'Offrant a obtenu tous les droits sur l'Oeuvre nécessaires pour pouvoir autoriser l'exercice des droits accordés par le présent Contrat, et permettre la jouissance paisible et l'exercice licite de ces droits, ceci sans que l'Acceptant n'ait aucune obligation de verser de rémunération ou tout autre paiement ou droits, dans la limite des mécanismes de gestion collective obligatoire applicables décrits à l'article 4(e);
- b. L'Oeuvre n'est constitutive ni d'une violation des droits de tiers, notamment du droit de la propriété littéraire et artistique, du droit des marques, du droit de l'information, du droit civil ou de tout autre droit, ni de diffamation, de violation de la vie privée ou de tout autre préjudice délictuel à l'égard de toute tierce partie.
- c. A l'exception des situations expressément mentionnées dans le présent Contrat ou dans un autre accord écrit, ou exigées par la loi applicable, l'Oeuvre est mise à disposition en l'état sans garantie d'aucune sorte, qu'elle soit expresse ou tacite, y compris à l'égard du contenu ou de l'exactitude de l'Oeuvre.

6. Limitation de responsabilité. A l'exception des garanties d'ordre public imposées par la loi applicable et des réparations imposées par le régime de la responsabilité vis-à-vis d'un tiers en raison de la violation des garanties prévues par l'article 5 du présent contrat, l'Offrant ne sera en aucun cas tenu responsable vis-à-vis de l'Acceptant, sur la base d'aucune théorie légale ni en raison d'aucun préjudice direct, indirect, matériel ou moral, résultant de l'exécution du présent Contrat ou de l'utilisation de l'Oeuvre, y compris dans l'hypothèse où l'Offrant avait connaissance de la possible existence d'un tel préjudice.

7. Résiliation

- a. Tout manquement aux termes du contrat par l'Acceptant entraîne la résiliation automatique du Contrat et la fin des droits qui en découlent. Cependant, le contrat conserve ses effets envers les personnes physiques ou morales qui ont reçu de la part de l'Acceptant, en exécution du présent contrat, la mise à disposition d'Oeuvres dites Dérivées, ou d'Oeuvres dites Collectives, ceci tant qu'elles respectent pleinement leurs obligations. Les sections 1, 2, 5, 6 et 7 du contrat continuent à s'appliquer après la résiliation de celui-ci.
- b. Dans les limites indiquées ci-dessus, le présent Contrat s'applique pendant toute la durée de protection de l'Oeuvre selon le droit applicable. Néanmoins, l'Offrant se réserve à tout moment le droit d'exploiter l'Oeuvre sous des conditions contractuelles différentes, ou d'en cesser la diffusion; cependant, le recours à cette option ne doit pas conduire à retirer les effets du présent Contrat (ou de tout contrat qui a été ou doit être accordé selon les termes de ce Contrat), et ce Contrat continuera à s'appliquer dans tous ses effets jusqu'à ce que sa résiliation intervienne dans les conditions décrites ci-dessus.

8. Divers

- a. A chaque reproduction ou communication au public par voie numérique de l'Oeuvre ou d'une Oeuvre dite Collective par l'Acceptant, l'Offrant propose au bénéficiaire une offre de mise à disposition de l'Oeuvre dans des termes et conditions identiques à ceux accordés à la partie Acceptante dans le présent Contrat.
- b. La nullité ou l'inapplicabilité d'une quelconque disposition de ce Contrat au regard de la loi applicable n'affecte pas celle des autres dispositions qui resteront pleinement valides et applicables. Sans action additionnelle par les parties à cet accord, lesdites dispositions devront être interprétées dans la mesure minimum nécessaire à leur validité et leur applicabilité.
- c. Aucune limite, renonciation ou modification des termes ou dispositions du présent Contrat ne pourra être acceptée sans le consentement écrit et signé de la partie compétente.
- d. Ce Contrat constitue le seul accord entre les parties à propos de l'Oeuvre mise ici à disposition. Il n'existe aucun élément annexe, accord supplémentaire ou mandat portant sur cette Oeuvre en dehors des éléments mentionnés ici. L'Offrant ne sera tenu par aucune disposition supplémentaire qui pourrait apparaître dans une quelconque communication en provenance de l'Acceptant. Ce Contrat ne peut être modifié sans l'accord mutuel écrit de l'Offrant et de l'Acceptant.
- e. Le droit applicable est le droit français.

Creative Commons n'est pas partie à ce Contrat et n'offre aucune forme de garantie relative à l'Oeuvre. Creative Commons décline toute responsabilité à l'égard de l'Acceptant ou de toute autre partie, quel que soit le fondement légal de cette responsabilité et quel que soit le préjudice subi, direct, indirect, matériel ou moral, qui surviendrait en rapport avec le présent Contrat. Cependant, si Creative Commons s'est expressément identifié comme Offrant pour mettre une Oeuvre à disposition selon les termes de ce Contrat, Creative Commons jouira de tous les droits et obligations d'un Offrant.

A l'exception des fins limitées à informer le public que l'Oeuvre est mise à disposition sous CPCC, aucune des parties n'utilisera la marque « Creative Commons » ou toute autre indication ou logo afférent sans le consentement préalable écrit de Creative Commons. Toute utilisation autorisée devra être effectuée en conformité avec les lignes directrices de Creative Commons à jour au moment de l'utilisation, telles qu'elles sont disponibles sur son site Internet ou sur simple demande.

Creative Commons peut être contacté à <http://creativecommons.org/>.