Guide de la

apatride

*

avril 2014

SOMMAIRE

introduction

Bonjour tout le monde !

Voici le **petit guide anarchiste de la vie privée sur internet**, le guide qui vous donne toutes les techniques et les infos à connaître pour enfin protéger votre vie privée lorsque vous vous connectez.

Ce guide ne s'adresse pas seulement à mes compañer@s anarchistes mais à tous celles et ceux qui s'intéressent un peu à la question. En fait, si tu as un PC et un accès internet, ça devrait t'intéresser puisque que globalement on est tous sur écoute...

Pour bien profiter de mes conseils, tu devrais d'abord installer un système libre sur ton PC si ce n'est déjà fait. Tu as l'embarras du choix parmi les systèmes GNU-Linux. Si tu débutes je peux te conseiller Linux Mint ou bien Trisquel qui est un système totalement libre. Même si j'utilise Ubuntu, je peux pas te conseiller cette distribution car elle n'est plus fiable depuis les dernières versions.

Ce pdf provient de mon site internet **apatride.noblogs.org**.
L'adresse complète pour retrouver le contenu de ce manuel est inscrite tout en bas sur les pages qui suivent.

amicalement

apatride

nov 14 2013

1. les extensions de firefox

Aujourd'hui, je vous propose un petit article sur la sécurité, parce qu'on est espionnés de partout, surtout sur internet.

Bon ça parait pas comme ça mais le navigateur a un rôle très important à jouer dans la protection de ta vie privée. Alors on va voir comment le configurer dans ce premier article.

Firefox est un navigateur libre qui a l'avantage de proposer de nombreuses extensions dans le domaine de la sécurité, alors c'est un bon choix pour commencer. Et il fonctionne sur windows, mac, linux. Au passage si tu tiens à ta vie privée laisse tomber Windows et mac.

Pour ajouter une extension à Firefox (ou encore module ou add-on), tu vas dans le menu Outils>Modules complémentaires, ce qui ouvre une page. En haut de cette page, tu peux utiliser la barre de recherche "Rechercher dans tous les modules". Quand tu as installé un module, en général firefox ajoute une petite icône dans l'interface, en haut ou en bas. Pour configurer une extension tu as le choix : soit en cliquant sur son icône et tu cherches "préférences", "options", ou une petite icône en forme d'engrenage... Soit depuis la page des extensions qu'on a vue juste au-dessus. Sur la gauche de cette page, tu choisis "Extensions" et tu cliques sur celle qui t'intéresse. Là aussi tu as un boutons "préférences", "options"... dans le genre.

Bon maintenant la liste des modules que j'ai installés et qui me paraissent vraiment utiles :

- **Adblock Plus** 

Bloquer les publicités et les trackers qui vont avec, et ça fait gagner beaucoup de temps dans l'affichage des pages.

Dans les préférences du module, tu choisis une liste de filtrage, la mienne c'est "Liste FR+Easylist".

Toujours dans les préférences, oublie pas de décocher "Autoriser certaines publicités non intrusives", c'est le créateur de l'extension qui essaie de se faire un peu de fric en loucedé.

- **Ghostery** 

Extension qui bloque les trackers, autrement dit les petits codes javascript planqués dans les pages web (il faut regarder la source de la page pour les voir) et qui récoltent

des infos sur toi. Et il y en a beaucoup !

Pour configurer ghostery, c'est pas compliqué. Dans les options (bouton engrenage) tu as trois onglets : "General", "Advanced" et "About". Dans l'onglet "General" tu coches tout à part le premier qui dit "Enable GhostRank", mais tu coches vraiment tout, même dans les onglets "Trackers" et "Cookies" en bas.

Dans l'onglet "Advanced", je te conseille de décocher "Show alert bubble" (ça soule au bout d'un moment). Puis – IMPORTANT – tu coches "Block new elements by default", et tu décoches" Notify me of new elements". Pour le reste tu peux tout cocher.

- **SettingSanity** 

Extension pas très connue et pourtant très utile.

Dans les dernières versions de Firefox apparemment, ils ont supprimé certaines options essentielles, comme le blocage automatique des images et du javascript. Cette extension te permet aussi d'ajouter des boutons dans l'interface. Quand tu bloques javascript, tu peux naviguer tranquillement car c'est vraiment de là que viennent les plus gros risques pour ta sécurité (virus et co) et pour ta vie privée. Si tu bloques javascript, ghostery ne sert plus à rien, mais bon c'est un peu radical car tu ne pourras plus regarder la plupart des vidéos en ligne par exemple.

A suivre…

no comments | posted in General, Un peu de vie privée

---

déc22013

2. configuration de Firefox

Dans ce post on va continuer la configuration de firefox, avec le réglage des préférences.

Donc ça se passe dans le menu de firefox : Editions>préférences

Beaucoup d'options à vérifier avec les différentes sections "Général", "Onglets", "Contenus" … c'est pas la partie la plus marrante, mais ça vaut le coup !

- **"Général"**

Rien qui concerne vraiment la sécurité, mais il arrive que Firefox soit "livré" avec

une page par défaut qui contient une barre de recherche Google. Je n'ai pas besoin de t'expliquer que ce moteur ne respecte pas du tout ta vie privée. Alors je te conseille de changer de page d'accueil avec celle-ci par exemple : https://startpage.com

En fait moi pour ma page d'accueil, j'utilise une extension qui s'appelle Super Start qui me permet d'accéder tout de suite à mes sites préférés, mais là c'est hors sujet.

- **"Onglets"** : rien de particulier

- **"Contenu"**

Coche "Bloquer les fenêtres pop-up" pour bloquer les pubs.

Là si tu as suivi mon conseil dans l'article précédent, tu as les options de l'extension SettingSanity. Tu peux modifier comme tu veux mais le plus simple c'est d'utiliser les icônes "fournies avec" dans l'interface. Mais elles sont pas affichées par défaut je crois. Pour les ajouter tu fais un clic droit sur une barre d'outils, qui peut se trouver en haut, à droite de la zone de recherche, ou en bas de firefox pour la "barre de modules". Il faut pas que tu cliques sur icône qui existe déjà, mais à côté ou entre deux icônes. Donc tu fais un clic droit et tu choisis "Personnaliser", et là tu pourras faire des changements dans l'interface. Les icônes pour SettingSanity ressemblent à ça :  pour javascript et  pour l'affichage des images.

- **"Applications"** : rien de particulier

- **"Vie privée"**

- Pistage : cette option ne sert pas à grand chose. Si tu demandes à Google ou aux sites de pubs de ne pas te suivre, ils te suivront quand même ! Tu peux choisir : "Ne rien indiquer aux sites" par exemple.

- Historique de navigation : à toi de voir ce qui te convient le mieux. Il vaut mieux choisir de vider les cookies à chaque fois que tu fermes Firefox pour éviter de te faire pister. Je te conseille aussi de ne jamais accepter les cookies qui proviennent de sites "tiers", c-à-d de sites que tu n'as pas toi-même visité.

- **"Sécurité"**

Tu coches tout ce qui est au-dessus de "Mots de passe".

Et pour les mots de passe tu peux choisir de les enregistrer, mais il te faut absolument un mot de passe principal, sinon ils sont visibles en clair par n'importe qui ! Il y a

beaucoup de mots de passe à enregistrer sur les différents sites. C'est conseillé d'utiliser un mot de passe différent à chaque fois. Pour pas te faire chier, utilise une extension comme Password Hasher, qui te permet de créer des mots de passe facilement en fonction du nom du site.

- **"Sync"**

Je ne l'utilise pas. Mais à mon avis c'est pas une bonne idée d'utiliser ce genre de service du point de vue de la sécurité.

- **"Avancé"**

Allé on y est presque !

- onglet Général : tu peux cocher "Prévenir lorsque des sites web tentent de rediriger ou de recharger la page" pour éviter les redirections automatiques.

- onglet Données collectées : ne rien cocher.

- onglet Réseau : cocher "Avertir lorsqu'un site souhaite conserver des données pour une utilisation hors connexion".

- Mises à jour : tu décoches

- Certificats : me demander à chaque fois

Voilà, on a fait le tour.

Pour finir, oublie pas d'ajouter **un bon moteur de recherche**.

Startpage est pas mal parce qu'il te permet d'avoir les résultats de google sans te faire pister.

Sur cette page :

https://startpage.com/eng/download-startpage-plugin.html

tu sélectionnes la bonne langue et tu choisis "Install" pour le HTTPS.

no comments | posted in General, Un peu de vie privée

---

jan142014

3. le VPN

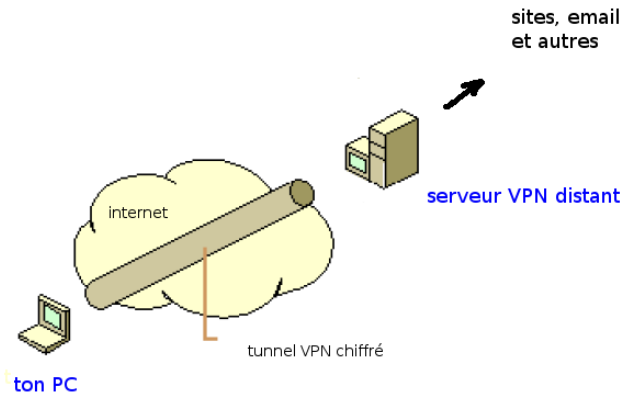
Salut

je vois qu'il y a un peu plus de gens qui passent sur le blog ce qui m'encourage à continuer. Hésitez pas à laisser des commentaires si vous avez un truc à dire, des remarques, des infos, des questions…

Aujourd'hui je continue dans la série "Vie privée" avec un sujet important : le VPN.

VPN signifie : Virtual Private Network – Réseau Privé Virtuel.

Quand on se connecte en VPN à un ordinateur ou un serveur (qui est aussi un ordinateur remarquez), c'est comme si on se connectait à un autre PC situé sur un réseau local et qui servirait d'intermédiaire entre toi et internet. La différence c'est que ce PC peut être situé au bout du monde et que la connexion est chiffrée (protégée) entre lui et toi. On appelle ça un tunnel VPN.



L'intérêt de cette technique c'est que ton fournisseur d'accès internet a aucun moyen de savoir sur quel site tu navigues ou avec qui tu chates par exemple. Et pareil pour les "services" de renseignement qui voudraient t'espionner directement.

OK ça tu le savais peut-être déjà, alors la question qui vient après c'est quel VPN choisir?

Des VPN il y en a des tonnes sur internet mais bon ils offrent pas tous les mêmes services et tu dois te demander aussi si tu peux leur faire confiance. J'ai un peu cherché de mon côté et je peux déjà t'en conseiller quelques uns :

- AirVPN

C'est celui que j'utilise. Il a plein d'avantages : il est pas très cher, genre 7€/mois mais ça dépend aussi de combien de mois tu choisis au départ. Tu as pas mal de serveurs répartis dans le monde entier et ils ne conservent aucune trace de tes activités sur

internet (pas de logs). Mais surtout il est géré par des activistes et des hacktivistes (hackers activistes) qui ont vraiment l'air honnêtes et sérieux. Ca se voit juste à la qualité de leur site et du support client. Il y a même un forum pour échanger avec les autres utilisateurs.

Si tu comprends l'anglais, tu peux lire cette page pour te faire une idée : About us

- VPN du site Autistici/Inventati

A/I c'est le site italien qui héberge le blog que tu es en train de lire. C'est des activistes eux-aussi mais qui n'ont aucune activité commerciale. Ils dépendent seulement des dons qu'ils reçoivent. Leur truc c'est de proposer tous les services possibles pour protéger la vie privée des militants et autres activistes radicaux : email, blogs, hébergement, VPN, … Je dois avouer que j'ai pas encore réussi à faire fonctionner leur VPN mais il y a pas de raison que ça marche pas. Par contre, comme ils le disent, c'est juste un VPN pour "dépanner", le débit est faible et il faut renouveler le certificat genre tous les 3 jours.

- D'autres VPN qui ont une bonne réputation : Ipredator, Private Internet Access, Boleh VPN, …

N.B.

Pour la plupart des VPN ci-dessus tu peux payer anonymement avec des bitcoins (monnaie virtuelle).

Dans le prochain post, j'expliquerai un peu les détails techniques pour faire fonctionner le VPN.

no comments | posted in General, Un peu de vie privée

---

fév132014

4. configuration du VPN

Suite de ma série sur la sécurité, toujours à propos du VPN.

Franchement si le sujet vous intéresse je vous conseille de relire mes posts dans l'ordre parce que les infos que je donne sont pas toujours faciles à trouver, en particulier pour la configuration du VPN dont je vais commencer à parler aujourd'hui. Je vais créer une catégorie spéciale 'vie privée' qui se trouvera dans le colonne de droite du blog.

Bon, si tu veux te familiariser avec le VPN, tu voudras peut-être un VPN gratuit pour commencer. Je peux te proposer la version gratuite de SecurityKiss qui t'offre 300Mo par jour et par compte, ça sera bien pour apprendre. J'en ai pas parlé dans le post

précédent parce que je me méfie un peu de ce genre de service gratuit, j'ai toujours l'impression qu'il y a une arnaque quelque part. Ils affirment effacer les données de navigation après 10 jours mais pourquoi les conserver de toute façon? en plus ils bloquent certains services comme le torrent.

Alors le premier truc à savoir : tu as **plusieurs protocoles possibles** pour le VPN. Les plus connus sont OpenVPN, PPTP, IPsec. **OpenVPN** est le meilleur du point de vue de la sécurité alors c'est celui que je vais présenter. Mais tu peux aussi choisir le PPTP qui est un peu plus facile à configurer.

Pour ajouter OpenVPN dans Network-Manager (qui ressemble à ça  en haut à droite de l'écran) il faut juste installer le paquet **network-manager-openvpn**. Après pour installer le VPN tout est expliqué ici en anglais. Il suffit de reproduire les commandes dans un terminal.

- Pour l'étape 0, tu t'arrêtes à la première commande si tu obtiens 1.
- Pour l'étape 1, il faut se connecter dans le panneau utilisateur sur le site de SecurityKiss, puis tu vas dans les onglets Download et Linux et tu cliques sur le bouton Download, ça prend un peu de temps… et tu décompresses l'archive.
- A l'étape 3, l'icône est différente mais sinon c'est pareil. La liste des serveurs est donnée dans le fichier README.txt, il suffit de copier/coller l'adresse IP de ton choix, tcp ou udp ça a pas beaucoup d'importance.

Voilà normalement tu es maintenant connecté en VPN depuis l'étranger (évite un serveur qui serait dans ton propre pays!). Tu peux le vérifier ici par exemple. C'est bon?

Je m'arrête là pour aujourd'hui. La prochaine fois je vous expliqueré comment régler le pare-feu, *muy importante*!

2 comments | posted in General, Un peu de vie privée

---

avr132014

5. régler le pare-feu pour le VPN

Salut à toi lecteur avide de connaissances nouvelles et libres

Aujourd'hui, poursuivons notre quête de vie privée avec ce dernier article à propos du VPN. Si tu m'as suivi jusque là, tu as appris le principe du fonctionnement d'un VPN, tu as découvert les VPN les plus recommandables et tu sais faire fonctionner un VPN gratuit sur ta machine linux. Bien! mais faut-il relâcher la pression pour autant? ça serait dommage car il manque encore une ultime étape pour que tout soit en place : le réglage du pare-feu.

Comme je te l'ai expliqué au début, le VPN se comporte comme une machine sur un réseau local. Autrement dit, quand tu te connectes à ton VPN, tu es en communication directe avec le serveur. Ton routeur (ta box par exemple) devient totalement transparent, c'est comme s'il n'existait plus. Il ne peut donc pas jouer son rôle de

filtre. Quand tu vas sur internet d'habitude, ta box te protège en bloquant toute tentative d'intrusion depuis l'extérieur, ce qui rend l'utilisation d'un pare-feu (firewall) pratiquement inutile. Mais dans le cas d'une connexion VPN, tu deviens vulnérable si tu ne penses pas à mettre en place le pare-feu.

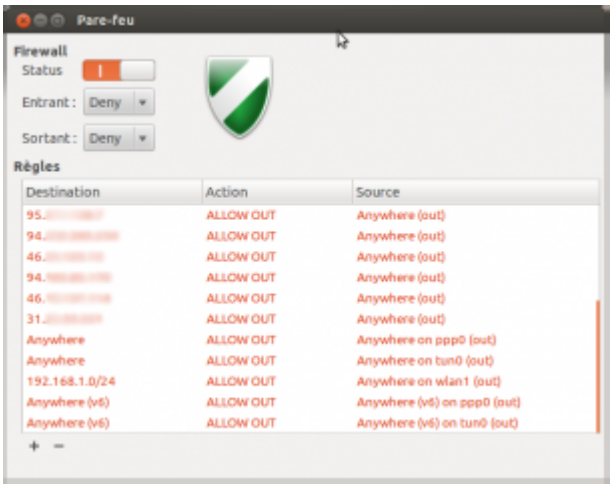
Par ailleurs, tu dois te demander : qu'est-ce qui se passera si je perds ma connexion VPN au beau milieu d'une session un peu "sensible" ? Hé bien la connexion qui passait par le VPN risque fort de se rétablir automatiquement sans VPN et tu te retrouves "tout nu" (vis-à-vis de ton fournisseur d'accès).

On a donc deux bonnes raisons de mettre en place un pare-feu et de le configurer comme il faut.

Sous linux, la gestion du pare-feu peut se faire simplement avec le logiciel ufw (uncomplicated firewall). Tu vas voir qu'effectivement c'est pas très compliqué à comprendre. Le logiciel ufw est installé par défaut sur certaines distributions. Tape **ufw –help** et tu verras ce qu'il te dit. Je te conseille d'installer en plus son interface graphique qui s'appelle gufw.

Configuration de ufw pour le VPN :

Ouvre un terminal et lance l'interface graphique gufw.



Tu verras un bouton 'Unlock' en bas à droite de la fenêtre. Tu dois cliquer dessus et entrer ton mot de passe administrateur.

La première chose à faire est de bloquer tout le trafic entrant et tout le trafic sortant sur ton ordinateur. Comme ça tu es vraiment protégé :) Pour ça, choisis 'Deny' dans les entrées Entrant et Sortant qui se trouvent en haut à gauche de la fenêtre. Après ça, tu as plus qu'à entrer les exceptions.

Ouvre un nouveau terminal.

D'abord il faut ajouter une autorisation pour tous les serveurs VPN que tu as l'intention d'utiliser. Il se peut qu'il y en ait qu'un, suivant le service VPN que tu utilises… Il faut que tu récupères son/leur adresse IP. Où ça? Hé ben normalement tu

as téléchargé les fichiers de configuration OpenVPN qui se terminent par l'extension .opvn. Tu ouvres ce/ces fichiers avec un éditeur de texte et tu auras dedans l'adresse IP du/des serveurs VPN, du genre 12.34.567.89.

Pour chaque adresse IP (une par serveur) tape la commande suivante :

sudo ufw allow out from any to 12.34.567.89

Pour chaque nouveau serveur, tu peux vérifier que la règle est bien enregistrée en appuyant sur la touche F5 dans gufw. En cas d'erreur, tu sélectionnes la règle dans la liste et tu cliques sur le bouton "-" qui se trouve en bas.

Tu peux maintenant te connecter à ces serveurs et communiquer avec eux.

Il faut maintenant ajouter une règle pour autoriser la communication à travers le tunnel VPN. La connexion au VPN crée une nouvelle interface réseau qui s'appelle tun0 ("tun-zéro").

Tu tapes la commande :

sudo ufw allow out on tun0 from any to any

Oublie pas de taper sur F5 pour que la régle s'affiche.

Et voilà, **c'est tout!** T'as plus qu'à lancer le pare-feu en cliquant sur le bouton 'Status' en haut à gauche. Statut : 1 actif, 0 inactif.

Quand tu fermes la fenêtre de gufw et même quand tu éteins ton PC, les règles et le statut on/off du parefeu sont sauvegardés, tu n'as plus à t'en occuper.

Bon, on a bien travaillé, on est bon pour cette fois.

Il y aura encore un dernier post dans cette série, dans lequel je vous diré tout ce que je vous ai pas encore expliqué sur le sujet…

Note :

Pour accéder au réseau local, pour accéder à la page de configuration de ta box notamment, tu auras besoin d'ajouter la règle suivante :

sudo ufw allow out on wlan0 from any to 192.168.1.0/24

J'ai mis wlan0 mais ça peut-être autre chose. Tu as la liste des interfaces réseau avec la commande **ifconfig**.

no comments | posted in General, Un peu de vie privée

---

avr142014

6. trucs en vrac

Salut,

Tant que je suis sur ma lancée, je vais tout de suite vous donner toutes les infos en plus qui sont bonnes à connaitre, mais juste pour vous donner des pistes, je vais pas tellement entrer dans le détail.

Fuites DNS

Le DNS c'est ce qui permet à ton ordinateur de savoir quelle adresse IP il doit faire correspondre avec telle adresse web, du genre bidule.com. Bon et ben en général c'est un service qui est géré par ton fournisseur d'accès à internet (FAI). Ce qui fait qu'à chaque fois que tu tapes une adresse dans ton navigateur, ça passe par le serveur DNS de ton fournisseur d'accès et il peut tout savoir des sites que tu as visité – plus de vie privée!

Pour éviter ça, il faudrait changer de serveurs DNS, ce qui est possible. Mais si tu utilises un bon service VPN, normalement tu devrais pouvoir échapper à cette étape. Si c'est bien fait, tu devré utiliser automatiquement un DNS intégré au serveur VPN. C'est ce qu'ils font chez AirVPN par exemple.

Sinon pour être certain qu'il y a pas de fuite tu peux essayer un site comme dnsleaktest.com

Pour voir, tu peux lancer un test sans vpn : tu devrais voir s'afficher des serveurs DNS de chez ton FAI.

Après ça, tu lances le VPN et tu recommences… et tu compares!

User-agent et compagnie

Il faut savoir que tous les paramètres de ton navigateur (tes préférences par exemple) peuvent permettre à un site que tu visites de te reconnaître, parce que ça t'identifie un peu comme une empreinte digitale. Pour ça malheureusement y'a pas grand chose à faire. Si tu veux voir à quel point tes paramètres sont uniques, tu peux faire le test sur le site Panopticlick. Tu verras, c'est un peu effrayant.

En fait, il y a qd même une solution, c'est d'utiliser un navigateur "pré-formaté", c'est-à-dire le même navigateur avec les mêmes réglages et le même user-agent (infos sur ton système) pour tout le monde. C'est exactement ce qu'ils font chez Tor. Tu connais pas Tor? eh ben t'as tort.

Tor Browser

Voilà, ça c'est le truc ultime ou presque pour rester anonyme sur internet. Je suis sûr que tu en as déjà entendu parler. Remarque qu'on parle d'anonymat pour Tor et pas juste de vie privée. Je ne vais pas t'expliquer le principe de Tor – renseigne-toi gros/se! – mais c'est le réseau utilisé par tous les hackers de la planète. Et pourtant c'est très facile à utiliser quel que soit ton niveau en informatique. T'as juste à télécharger le kit ici et tu te laisses guider.

Mais si c'est si simple, pourquoi tu m'en as pas parlé plus tôt?? eh bien tu as raison j'auré pu mais en même temps Tor n'est pas fait pour la navigation de tous les jours. Il y a plein de choses que Tor ne permet pas et il bloque des plugins vraiment très présents sur le web comme le flash par exemple. En plus de ça, la navigation est franchement ralentie. Alors utilise-le seulement si tu veux être sûr de protéger ton anonymat, parce que ça il le fait très bien.

Par contre, un conseil : n'entre pas des données personnelles en utilisant Tor (comme un mot de passe) par ce que ça pourrait être intercepté au passage par un nœud malveillant (la NSA? qui a dit la NSA?).

Et pour les mails??

Les mails, laisse tomber c'est un mauvaise idée

Soit tu utilises un service en ligne comme il y en a des milliers mais tu sauras jamais ce qu'ils font de tes mails. Soit tu installes toi-même ton serveur mail sur ton PC : truc de geeks… En plus il parait que les mails peuvent se copier sur tous les serveurs par lesquels ils transitent.

Il parait aussi qu'on peut chiffrer ses mails quand on les envoie. OK mais ça nous avance pas beaucoup…

Le mieux à mon avis c'est de chatter directement avec les gens. Enfin pas sur Skype évidemment, on peut pas leur faire confiance. Ni sur IRC parce que ça laisse des traces. Il doit exister des logiciels pour chater directement sans intermédiaire, il faudrait que je me renseigne…

Sinon

Sinon, tu jettes ton PC bien sûr !!

Bon en tout cas je pense que je vous auré donné une bonne vue d'ensemble sur le sujet.

Faites-en ce que vous voudrez, et si vous avez une suggestion ou un commentaire à faire, je vous écoute!

FIN

no comments | posted in General, Un peu de vie privée

Subscribe RSS
'Proudly powered by R*'