Compte-rendu des Rump-sessions SSTIC 2007

rédigé le 6 juin 2007 par Bruno Kerouanton (*http://bruno.kerouanton.net*)

RCJU / SDI - rue de la Justice 2 - 2800 Delémont, Suisse

Résumé : Cette année apportait son lot de records. Rapidité d'inscription, nombre de participants, mais également nombre de rumps lors des 5ème Rump-Sessions du SSTIC. Du coup, l'organisateur de cette session, Franck Veysset, a eu le plus grand mal à canaliser la horde de personnes venant à lui pour lui demander d'ajouter une ligne à la déjà dense liste des rumps.

Comme les années précédentes, le sujet était libre, sous réserve que cela ait un rapport avec la sécurité des systèmes d'information. La durée de chaque présentation étant limitée à 4 minutes pour pouvoir laisser s'exprimer chaque personne inscrite.

De très bons sujets, des innovations et présentations percutantes, et plusieurs sujets assez décalés, car comme la tradition le veut l'humour est de mise lors des rumps du SSTIC !

Table des matières

Compte-rendu des Rump-sessions SSTIC 2007....1
0) Infos diverses : Annonce CESAR / CELAR....2
00) Nicolas Fischbach && Fred Raynal : SSTIC 5.0....2
1) Victor Stinner : Fuzzing de fichier....2
2) Lieutenant Mohamed Ould Salem : Les enjeux de la SSI pour l'Armée Nationale Mauritanienne....3
3) Olivier Levillain :NEwspeak, un langage pour l'analyse statique de code....3
4) Nicolas Grégoire : la faille mod_jk (CVE-2007-0774)....3
5) Fabrice Mourron : l'interface graphique de Metasploit v3....4
6) Julien Cayssol : l'outil revhosts....4
7) Eric Filiol : résultats d'évaluation de OneCare....4
8) Guillaume Lehembre : RainbowTables et caractères accentués sous Windows....5
9) Christophe Grenier : Récupération de données cachées dans des CDROMS....5
10) Stéphane Jourdois : Petit Trojan hardware....5
11) Sébastien Tricaud & Pierre Chifflier : Prelude IDS....6
12) Gera : Crypto Stuff / heap massage....6
13) Alexandre Cabrol-Perales : Présentation de l'ADSSI....6
14) Vincent Guasconi & Shengjie Zhan : Bugs et/ou failles....6
15) Nicolas Brulez : Le debugging furtif sous Windows....7
16) Thomas Sabono : Fiabilité des logiciels antirootkit sous Windows 32 bits....7
17) Bruno Kerouanton : Cyberguerre....7
18) Guillaume Valadon : Scapy 6.0....7
19) Phil Biondi : Graphes 3D....8
20) Guillaume Arcas : tHTP....8
21) Benjamin Caillat : Wishmaster....9
22) Tim Burrell, Microsoft : Un exemple d'analyse statique....9
23) Renaud Feil : Chiffrement over HTTP....9
24) DJ Julien, Raph et Yoann : Elektronik Supersonik....9
Document changes....10

0) Infos diverses : Annonce CESAR / CELAR

Comme l'année dernière, avant d'entrer dans le vif du sujet, un peu de temps était prévu pour les annonces diverses. La première, comme l'année dernière, était une annonce pour les prochaines journées du CELAR (Anciennes JSSI, à ne pas confondre avec les JSSI de l'OSSIR très intéressantes également, mais se déroulant sur Paris).

Les journées du CELAR, se dérouleront du 6 au 8 novembre 2007 à Bruz près de Rennes. Chaque année aborde un thème différent, et 2007 sera consacré à la cryptographie. L'appel à contribution est ouvert jusqu'au 15 juin, si certains ou certaines maîtrisent le sujet, n'hésitez pas.

Eric Filiol a également tenu au nom de la communauté scientifique à exprimer ses félicitations pour les travaux de Xavier Allamigeon et Charles Hymans, ainsi que la présentation qui nous en a été faite le matin même, concernant l'analyse statique par interprétation abstraite. En effet il s'agit d'un travail de recherche vraiment abouti et novateur, et devraient apporter une plus value significative dans les prochaines années pour contribuer à renforcer la sécurité des développements.

- Journées CESAR : http://www.rennes.supelec.fr/JSSI/
- X. Allamigeon et C. Hymans : http://www.lix.polytechnique.fr/Labo/Xavier.Allamigeon/

00) Nicolas Fischbach && Fred Raynal : SSTIC 5.0

Après leur excellente et hilarante rump d'introduction de l'année dernière, Nico et Fred ont tenté un remake, en nous présentant leur vision de SSTIC v5.0.

Quelques private jokes sur les célèbrités et personnes incontournables du SSTIC, avec photos (compromettantes... ou pas) à l'appui, un rappel de la composition de la salle comme l'année précédente (avec deux ajouts : les « touristes », et les « vraies filles »...), et une révélation : le SSTIC est non seulement un lieu d'enrichissement technique, mais surtout un lieu de rencontre, le mythe « *MeeSSTIC* » est donc né !

Ce petit remake sentait néanmoins le réchauffé car reprenant des éléments de l'année précédente et bien qu'amusant, n'a pas eu un impact percutant pour les habitués du SSTIC.

- SSTIC http://www.sstic.org

1) Victor Stinner : Fuzzing de fichier

Après les formalités d'introduction, nous voici donc plongés dans les « vraies rumps », avec tout d'abord un sujet d'actualité, le fuzzing. Technique brutale et souvent méprisée par les puristes, car automatisant les tests d'injection de données diverses et variées au niveau des entrées de programme jusqu'à ce qu'il plante, preuve qu'une faille potentielle s'y cache...

Fusil est donc un outil de fuzzing permettant de torturer les applications jusqu'à ce qu'elles cèdent. Il est écrit en *Python*, langage vraiment en vogue pour tout ce qui est « bricolage » de

données. Son mode de fonctionnement est assez simple : il prend un ou des fichiers de données en entrée et en modifie leur contenu avant de les transmettre à l'application, et teste le résultat...

Assez efficace à en juger par la liste des programmes cassés avec *Fusil*,et nous avons même eu le droit à une petite démonstration.

- L'outil de fuzzing *Fusil* : http://fusil.hachoir.org/

2) Lieutenant Mohamed Ould Salem : Les enjeux de la SSI pour l'Armée Nationale Mauritanienne

Deux officiers de l'Armée Nationale Mauritanienne nous ont ensuite présenté leur pays que nombre d'entre nous ne connaissaient que de nom, situé au sud du Maroc, très vaste et aux frontières immenses.

Compte-tenu de son histoire (la Mauritanie étant colonie française avant de proclamer son indépendance en 1960), les relations entre les deux pays restent privilégiées. En décrivant le passé et le mode de vie du peuple mauritanien, ainsi que les risques et enjeux militaires du pays, le lieutenant nous a interpellé sur l'évolution des systèmes d'information et des préoccupations en découlant dans le domaine de la sécurité.

Une rump que j'ai appréciée, notamment grâce à plusieurs citations locales telles que "Les hommes pressés sont déjà morts" prêtant à la réflexion et au recul.

- Lien Wikipédia : http://fr.wikipedia.org/wiki/Mauritanie

3) Olivier Levillain :NEwspeak, un langage pour l'analyse statique de code

Après nous avoir le matin même présenté les excellents travaux d'analyse statique par interprétation abstraite, il nous fallait tout de même quelque chose de concret, ce que les auteurs ont fait.

Le langage NEwspeak conçu pour l'occasion permet de transformer un code source C en code source NEwspeak, plus facile à traiter par la suite si l'on cherche à en effectuer une analyse statique. Des exemples sont présents sur le lien qui suit.

- Langage NEwspeak : http://www.penjili.org/newspeak.html

4) Nicolas Grégoire : la faille mod_jk (CVE-2007-0774)

Nicolas nous a fait la démonstration de la faille présente dans Apache Tomcat et plus précisément du module mod_jk. L'intérêt de la rump était que *Nicob* a réalisé un exploit multiversions, en utilisant une dll tierce compilée pour l'occasion sans l'option SafeSeh et permettant donc de prendre le contrôle du serveur quelque soit la version installée...

- Avis concernant la faille : http://www.frsirt.com/bulletins/9372

5) Fabrice Mourron : l'interface graphique de Metasploit v3

Metasploit est devenu l'outil incontournable des pentesteurs. Il est assez exceptionnel et fonctionne via ligne de commande ou interface web. Mais il lui manquait une interface graphique.

C'est chose faite en GTK (c'est fou tout ce qu'on peut interfacer avec Ruby !) et la démonstration de l'interface, bien qu'un peu longue à démarrer ce qui a suscité l'hilarité dans la salle, était intéressante : un vrai « *wizard* » à la Windows, avec son lot de boutons « suivant » permettant de prendre le contrôle d'un serveur en trois clics...

A quand un bouton : « hack the planet » ? a t'on demandé dans la salle... Dans la prochaine version, répondirent les auteurs avec humour !

- Interface et captures d'écran : http://laramies.blogspot.com
- Excellente vidéo de l'outil en action : http://fab.revhosts.net/files/msfassistant/msfassistant.html

6) Julien Cayssol : l'outil revhosts

Présentation de Revhost de OiaTeam. Tous les pentesters le savent, un bon outil d'énumération des serveurs présents sur le réseau testé est indispensable.

Revhosts 2.0 est un outil écrit en Python (encore et toujours !) permettant de trouver par différents moyens les serveurs d'un domaine. Interrogations DNS, scans, voire même interrogation des moteurs de recherche, tout y passe.

Un outil assez précieux donc pour les personnes en charge des tests sécurité.

- Outil et vidéo de démonstration : http://www.revhosts.org

7) Eric Filiol : résultats d'évaluation de OneCare

Eric Filiol, expert reconnu dans le domaine de la virologie, a présenté ses résultats d'évaluation de l'antivirus Microsoft OneCare. Une présentation en 4 slides : installation, parmétrage, fonctionnement, conclusion. 4 slides au contenu éloquent :

- Installation oui, mais il faut obligatoirement un accès à Internet, et tant pis pour les PC isolés.

- Paramétrage oui, mais juste un bouton « marche/arrêt », il ne faut pas trop en demander tout de même !

- Fonctionnement : un peu mieux (28% de détection) que Norton (26% de détection) face à Kaspersky (100% des virus détectés)... Ce slide a suscité la polémique durant la soirée, beaucoup de personnes s'interrogeant sur la provenance de ladite base, qui pourtant provient d'un site indépendant : site vx.netlux.org, et n'est en aucun cas affilié à l'un ou l'autre des éditeurs anti-virus. Ces chiffres démontrent simplement que le nombre de signatures prises en compte par les différents anti-virus ne sont pas les mêmes.

Enfin le dernier slide avec sa fameuse conclusion, qui a fait rire beaucoup de monde : la réponse d'un cadre européen de Microsoft, proche de ceci : « Microsoft prend la sécurité au sérieux mais n'est de toute manière pas une société de sécurité ». Laconique !

- Eric Filiol : http://fr.wikipedia.org/wiki/%C3%89ric_Filiol
- OneCare : http://onecare.live.com

8) Guillaume Lehembre : RainbowTables et caractères accentués sous Windows

Depuis que Philippe Oechslin a popularisé la notion de « *Rainbow Tables* », et que certains outils se diffusent plus vite que les pandémies, tout le monde se met à casser des mots de passe.

Le hic est que les tables générées sont très souvent d'origine anglo-saxonnes et ne prennent pas en compte la majorité de nos spécialités régionales, à savoir les caractères accentués, ou plus simplement le signe € voire même des caractères unicode quasi-standard. HSC a pourtant besoin lors de ses audits de casser du mot de passe franco-français avec ses cédilles et ses accents.

Ils ont alors patché les tables rainbow existantes à l'aide d'un outil maison pour prendre en compte les différentes accentuations de chaque voyelle. Ce sont donc les seuls (pour le moment) capables de casser de tels mots de passe.

- Rump : http://www.hsc.fr/ressources/presentations/sstic07_rump_rainbow/index.html.fr

9) Christophe Grenier : Récupération de données cachées dans des CDROMS

L'année dernière, Christophe Grenier nous avait déjà présenté son outil de récupération de données, Photorec, sous licence Open Source. Celui-ci est capable de retrouver les fichiers effacés ou corrompus présents sur de nombreux supports et systèmes de fichiers, et il a subi quelques récentes modifications lui permettant également de lire les CD-Roms (extensions Joliet, RockRidge etc.).

Outre la capacité de l'outil à récupérer les fichiers corrompus sur des CD et DVD, celui-ci lit également les fichiers cachés : Certaines personnes malignes utilisent le format multi-sessions de manière particulière pour dissimuler des fichiers, en ouvrant une nouvelle session sans avoir refermé l'ancienne ou en utilisant les possibilités « d'effacement de fichier » qui n'effacent en fait rien mais masquent leur présence.

Photorec est par conséquent capable de retrouver ces documents, intéressante initiative pour les spécialistes en recherches de preuves informatiques et experts judiciaires.

- Photorec : http://www.cgsecurity.org/wiki/PhotoRec

10) Stéphane Jourdois : Petit Trojan hardware

L'originalité du cheval de troie présenté par Stéphane Jourdois était son aspect. Un petit serveur Linux branché derrière le PC au niveau de la carte réseau, interçeptant et modifiant les flux à la volée pour pouvoir sortir des informations sur Internet malgré les proxies avec authentification NTLM. Intéressant concept, mais un souci concernant la furtivité de la méthode, l'alimentation du micro-serveur étant plus volumineuse que ce dernier. Mais comme il nous l'a bien rappelé, lorsqu'un utilisateur voit des cables traîner derrière son PC, en général il n'ose pas les débrancher !

- Micro-serveur Linux : http://www.gumstix.org

11) Sébastien Tricaud & Pierre Chifflier : Prelude IDS

Une introduction à Prélude-IDS, cet ensemble réunissant l'ensemble des fonctionnalités que l'on est en droit d'attendre d'un NIDS/HIDS (aussi appelé IDS hybride) distribué avec corrélation de logs et plein de bonnes fonctions. A noter : son créateur, Yoann Vandoorselaere, était présent et a créé sa société pour le support de Prelude.

- L'outil : http://www.prelude-ids.org

12) Gera : Crypto Stuff / heap massage

Une petite rump très visuelle dans le domaine de la rétroconception, ou plus précisément de l'exécution dynamique de programmes sous IDA Pro avec visualisation en temps réel et sous forme graphique de la « Heap » lors du fonctionnement d'application. Gera, de Core Security a donc réalisé cet excellent plugin IDA, dans le but de trouver (et d'exploiter) des failles dans les dernières versions de Windows.

La démonstration était ludique, on voyait bien l'affichage de la mémoire, les breakpoints, la Heap Windows et les malloc() mfree() en temps réel, permettant de se positionner judicieusement pour lancer l'exploit. Dommage que Gera ait du abréger, son temps de parole étant écoulé.

- Site de Core Security : http://community.corest.com
- Ida Pro : http://www.datarescue.com

13) Alexandre Cabrol-Perales : Présentation de l'ADSSI

L'association pour le Développent de la Sécurité des Systèmes d'Information en est à ses débuts. Lancée dans le but d'assister les PME et petits organismes incapables de se payer un RSSI, mais également les écoles et autres institutions, l'ADSSI est en phase de recherche de sponsors et de bénévoles pour augmenter son réseau national et ses actions.

Elle a déjà un parrain reconnu en la personne d'Eric Filiol, et toutes les personnes dans la salle semblait souhaiter le succès et la longue vie à cette association.

Outre ses actions de sensibilisation, elle est également reconnue comme organisme de formation et ne devrait pas tarder à dispenser des cours dans le domaine de la SSI à destination des élèves, des artisans et autres acteurs à sensibiliser d'urgence.

- Site de l'ADSSI : http://www.adssi.fr

14) Vincent Guasconi & Shengjie Zhan : Bugs et/ou failles

Présentation assez polémique : La faille des navigateurs web qui existe depuis 7 ans et qui permet de récupérer /etc/passwd en une seule commande... Beaucoup de monde a cru à un canular (dont moi), et le soir venu, le Social Event a été l'occasion d'en reparler. Je reste indécis, malgré ce qui se dit sur certains blogs...

- http://altmylife.blogspot.com/2007/05/rump-sessions-sstic-2007-demo-compose.html

15) Nicolas Brulez : Le debugging furtif sous Windows

Nicolas Brulez, l'as français du reverse-engineering et de la protection x86, a concocté un déboggeur-furtif-polymorphique-chiffré totalement écrit en assembleur (cela va de soi de la part de Nicolas), afin de déjouer les protections les plus tenaces.

D'après lui tout y passe : Armadillo 4, et même la meilleure protection commerciale du moment mettant en jeu une quantité impressionnante de contremesures... Bien entendu, cet outil restera sagement dans les coffres-forts de son employeur WebSense.

Ce qui est intéressant à savoir, c'est qu'il a conçu cet outil car de plus en plus de malwares se promennent sur Internet avec des protections ultra sophistiquées, leurs auteurs n'hésitant pas à acheter des outils de protection commerciaux (avec des numéros de cartes bleues volées), dans le but de rendre fous les chercheurs en virologie qui mettent au point les signatures et tentent de comprendre les fonctionnalités de ces malwares. D'où la nécessité de développer un tel débogueur.

16) Thomas Sabono : Fiabilité des logiciels antirootkit sous Windows 32 bits

Petite rump intéressante démontrant par A+B qu'il est très simple de conçevoir des rootkits sous Windows totalement indétectables. Preuve à l'appui avec un tableau présentant les principaux anti-rootkits du marché et leur capacité à détecter (ou pas) différentes choses suspicieuse.

Ne voulant pas vous induire en erreur en vous narrant des énormités, je n'en dirai pas plus faute d'avoir été attentif, mon tour venant ce qui a nui à ma concentration...

17) Bruno Kerouanton : Cyberguerre

Après une rapide petite annonce, cette rump traitait de la première Cyberguerre déclarée comme telle ayant eu lieu fin avril 2007 entre l'Estonie et la Russie, cette dernière ayant vraisemblablement lancé une attaque massive en déni de service distribué via des réseaux de bots (botnets) visant à saturer l'ensemble des sites gouvernementaux, de médias et d'acteurs principaux estonniens.

Cette série d'attaques a duré près de 3 semaines, au point que la Commission Européenne et même l'OTAN s'en sont inquiétés... Cela démontre en tout cas que cela n'est plus de la fiction, et qu'il va bien falloir s'attendre à ce qu'un jour ou l'autre ces pratiques arrivent... Au moins cela ne fait pas de morts (pour le moment).

- Rump : http://bruno.kerouanton.net/papers/sstic2007-mai07-bk-cyberguerre.pdf

18) Guillaume Valadon : Scapy 6.0

Il n'est plus besoin de présenter Scapy, le fameux outil écrit en Python par Phil Biondi (c'est lui qui

a lancé la mode de ce langage au sein de la communauté SSI !)... et fabuleusement documenté :)

Une nouvelle version est désormais capable de faire la même chose en Ipv6...

- L'outil : http://namabiiru.hongo.wide.ad.jp/scapy6

19) Phil Biondi : Graphes 3D

Au début, personne ne savait où Philippe Biondi, l'auteur de Scapy cité précédemment, voulait nous mener. Il y avait à l'écran une simple xterm sur fond de X11, sans aucun window manager... Puis quelques commandes plus tard, une fenêtre noire s'ouvre avec des boules de couleur qui tournent... Isocaèdre, pyramides, et autres formes 3D. Un coup de souris pour secouer les boules et perturber le mouvement naturel.

Amusant certes, mais sans rapport avec la sécurité, ni même le monde de Scapy et des réseaux. Puis la première commande intriguante arriva : un traceroute sous Scapy avec chaque boule affichée représentant un noeud. Au fur et à mesure des commandes saisies (via Scapy, of course) et des explications de Phil, des réseaux entiers s'affichent dans l'espace, des détails s'affichent sur les noeux, des sphères clignotent en indiquant que tel ou tel port est ouvert... Et tant qu'à faire de la 3D, une option stéréoscopie permet de voir le tout en relief avec les fameuses lunettes aux filtres rouge-bleu...

Un seul mot : fascinant !

Sa rump a fait du bruit, on en a entendu parler durant toute la soirée, le lendemain tout le monde essayait les lunettes 3D et de nombreux blogs en reparlent, il y a de quoi. A propos, j'ai téléchargé les sources : c'est forcément écrit en... Python !

- Magnifiques captures d'écran et outil ici : http://www.secdev.org/projects/ipv6world/

20) Guillaume Arcas : tHTP

Si vous avez fait des réseaux, vous connaissez les RFC, ces documents officiels présentant la normalisation de tout ce petit monde. Et si vous êtes mordus, la RFC 1149 ne vous est pas inconnue...

Cette rump propose une amélioration de la RFC 1149 en y ajoutant du chiffrement, un transport de paquets plus important et d'autres choses sympathiques...

Après la description technique et même les études concernant les contremesures associées, nous avons eu le droit à uune démonstration pratique du protocole, appelé à juste escient et avec malice « mooSSTIC » !

Afin de ne pas vous gâcher la surprise, je vous laisse ici le lien vers la présentation.

- Rump : http://yom.retiaire.org/lib/exe/fetch.php?id=le_sstic_est-il_toujours_le_sstic&cache=cache&media=start:thtp.pdf

21) Benjamin Caillat : Wishmaster

Wishmaster est un outil de génération de shellcodes à la volée. En quelques commandes vous avez le shellcode que vous voulez, préparé pour la plate-forme que vous aller attaquer, et c'est assez efficace. Je ne suis pas fan de ce genre d'outils n'en ayant pas l'utilité mais il semble très puissant, et certains chevaux de troie (Parsifal, ...) s'en servent avec succès.

- Lien vers l'outil : http://benjamin.caillat.free.fr/wishmaster.php

22) Tim Burrell, Microsoft : Un exemple d'analyse statique

Afin de nous montrer que Microsoft n'est pas si mauvais qu'on le dit, Tim Burell, employé de la firme, nous a présenté les méthodes d'analyse statique des codes que les développeurs de Microsoft conçoivent.

Il s'agit de désassemblage et d'analyse automatique de certains critères permettant assez rapidement de se faire une idée de la qualité du code écrit... et par déduction du développeur.

Tim Burrell a ensuite expliqué que cela servait au contrôle qualité, à l'évaluation puis à la prise en compte des erreurs afin de « corriger le problème »... Je crois qu'il y a eu un gros doute dans la salle à ce sujet à ce moment, personne ne sachant vraiment si il parlait des mauvais développeurs ou des mauvais programmes, ce qui en terme d'avancement de carrière (ou de carrière tout court) n'est pas du tout pareil !

23) Renaud Feil : Chiffrement over HTTP

L'avant-dernière rump était présentée par HSC, et tout comme l'année précédente se focalisait sur les possibilités d'attaquer directement le poste client... en HTTP. Après-tout pourquoi pas ?

L'utilisation de code polymorphique et d'obfuscation de fonctions de chiffrement, le tout en Javascript (si, si !), permettait de démontrer que l'on pouvait leurrer proxies filtrants et IDS tout en affichant des choses sur le navigateur distant. Un peu tordu comme concept, mais bon, nous étions au SSTIC !

24) DJ Julien, Raph et Yoann : Elektronik Supersonik

Et la meilleure rump était naturellement pour la fin ! De l'art de l'utilisation des stagiaires à des fins non productives mais néanmoins didactiques et à caractère hilarant.

Tout d'abord la présentation d'une petite vidéo (que tout le monde attend avec impatience) et qui, en faisant le tour des bureaux de ces trois sympathiques personnages, nous montre leurs occupations au quotidien : la préparation de quelque sujet intéressant pour le SSTIC : un article pour MISC, un fignolage de « remote kernel Linux » (sic !), et enfin le meilleur, le travail du stagaire...

Un rafistolage grossier reliant boîtes en carton, disques durs (sans couvercle),filasses colorées allant des uns aux autres, cartes électroniques aux soudures grossières, amplificateur 8W fait

maison... Bizarre bizarre... tout au long de la vidéo, une petite musique lancinante se répète incessament.

Gros plan sur les plateaux tournant des disques durs, et leurs têtes de lecture s'affolant dans un va-et-vient endiablé. La musique semble plus proche. Le doute n'est plus possible, ce sont bel et bien les têtes de lecture et les plateaux qui font cette musique, les boîtes en carton sous-jacentes faisant office de caisse de résonance et le microcontrôleur servant à réguler les têtes de lecture en fonction de la fréquence souhaitée.

Et oui, ils l'ont fait ! De la musique avec des têtes de lecture de disques durs... Certes, ce n'est pas une innovation en soi car cela avait été réalisé auparavant, mais bon, c'est toujours sympathique et cela suscite la curiosité admirative.

Les rump-sessions étant finies, nous avons eu la chance de pouvoir admirer le prototype de plus ou moins près, un importante foule s'étant rapidement massée autour de l'engin pour en admirer la subtilité et satisfaire sa curiosité tout en en faisant bénéficier son ouïe plus ou moins exercée.

Document changes

v1.0 : version initiale

v1.1 : corrections mineures