SSTIC 2015

Compte-rendu

Guillaume Lopes
Consultant Sécurité
Guillaume.Lopes@intrinsec.com

Plan

IntroduSSTIC

SSTIC

- Conférence de sécurité se tenant à Rennes
  - 13ème édition
  - S'est déroulée sur trois jours, du 3 au 5 juin 2015
- Programme
  - 30 présentations
  - 33 rumps
  - Annonce des résultats et présentation de la solution du challenge SSTIC
- Social event le jeudi soir à la Halle Martenot

Plan

Quelques chiffres

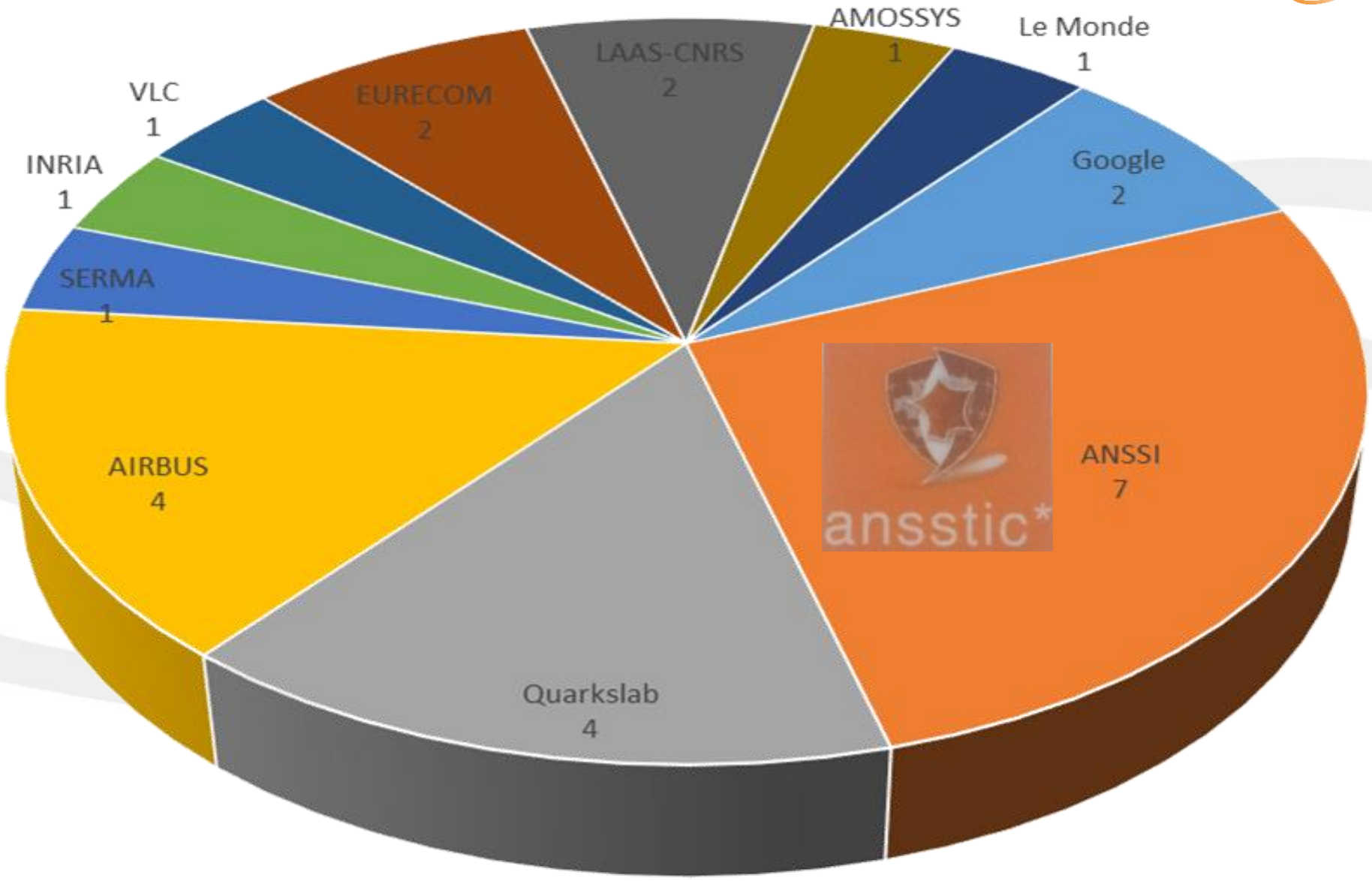
Quelques chiffres

- 450 participants !
  - Un amphi complètement rempli
- 320 places ont été vendues lors de la 1ère vague en 153 secondes
  - Ce n'était pas prévu…
- 19 soumissions courtes
- New high scores !
  - 77 heures pour résoudre le challenge
  - 94 pages dans les actes pour une conférence (consoles de jeux)
  - 480 pages pour les actes

Quelques chiffres

- Un mini-challenge était caché dans les actes !
- Le gagnant peut pré-réserver sa place pour l'année prochaine ☺
  - Il faudra quand même la payer
- Trop tard pour participer, il a été résolu pendant le SSTIC

Quelques chiffres



Plan

Jour 1

- ✓Mon TOP 3
  - ✓Sécurité et ingénierie dans Chromium
  - ✓Stratégies de défense et d'attaque : les cas des consoles de jeux
  - ✓Rétro-ingénierie matérielle pour les reversers logiciels : cas d'un DD externe chiffré

Jour 1

- Sécurité et ingénierie (dans Chromium) par Julien Tinnès
  - Julien est membre de l'équipe sécurité de Chromimum
  - Vision sur l'évolution de la sécurité depuis 2005
  - Présentation de quelques fonctions de sécurité sur Chromimum
    - Privilege isolation
    - Sandboxing
    - Seccomp-bpf
  - Présentation des fonctions de sécurité de ChromeOS
  - Nécessité de lier l'ingénierie logicielle et l'ingénierie sécurité
    - Dans de nombreux cas, la sécurité implique la qualité

Equipe sécurité de Chromium

Jour 1

- PICON : Control Flow Integrity on LLVM par Thomas Coudray, Arnaud Fontaine et Pierre Chifflier
  - Protect Integrity of CONtrol flow
  - Conception d'un outil permettant de limiter les possibilités d'exploitation de failles
  - Concept : vérification de l'intégrité du flot d'exécution
  - Mise en œuvre
    - Protéger tous les appels de fonction et les retours de fonction
    - Protéger les branchements
    - Détecter dès que possible si le flot d'exécution est compromis afin de terminer le programme
    - Disposer d'informations pour une analyse forensique
- Pour tester l'outil : https://github.com/ANSSI-FR/picon
  - Enfin… on attend toujours la publication

Jour 1

- Triton : Framework d'exécution concolique par Florent Saudel et Jonathan Salwan
  - Projet de fin d'études
  - Framework d'exécution concolique
    - Concolique = exécution concrète (dynamique) et exécution symbolique (analyse statique)
  - L'outil est disponible sur Github : https://github.com/JonathanSalwan/Triton

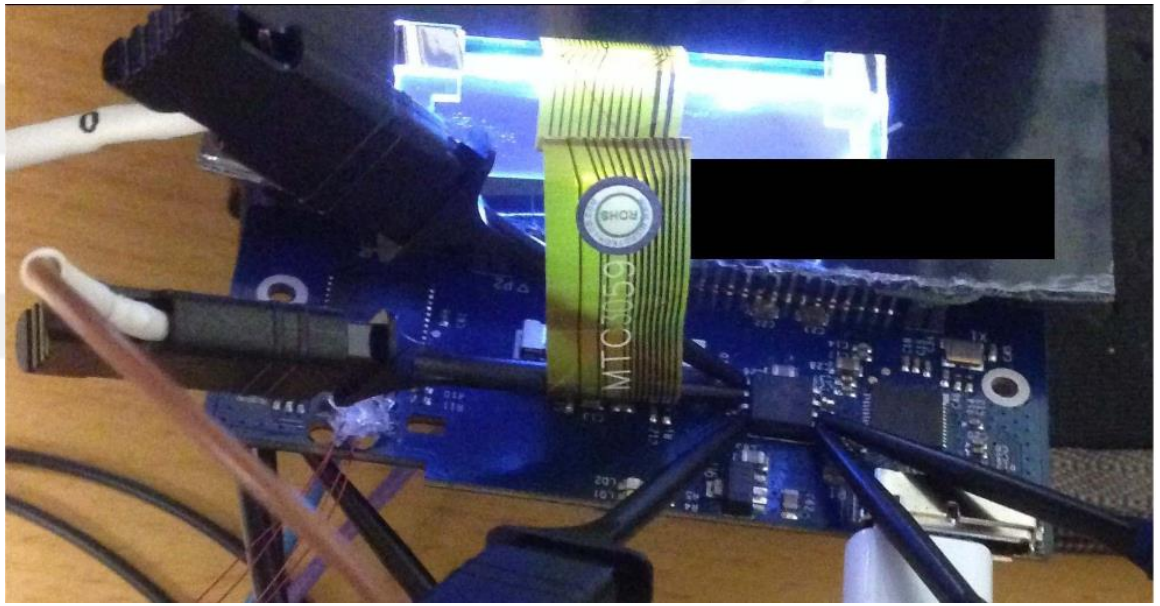
- REbus : Un bus de communication facilitant la coopération entre outils d'analyse de sécurité par Philippe Biondi et Xavier Mehrenberger
  - Outil permettant d'automatiser l'exécution d'outils d'analyse
  - REbus est disponible ici : https://bitbucket.org/iwseclabs/REbus
  - Une démo est disponible ici : https://bitbucket.org/iwseclabs/REbus_demo

Jour 1

- Abyme : un voyage au cœur des hyperviseurs récursifs par Benoît Morgan, Eric Alata, Guillaume Averlant et Vincent Nicomette
  - Est-il possible de réaliser un hyperviseur « récursif » ?
  - Permet d'isoler les composants d'une machine
  - Les performances ne sont pas au rendez-vous
- Stratégie de défense et d'attaque : le cas des consoles de jeux par Mathieu Renard et Ryad Benadjila
  - Présentation de la sécurité dans les consoles de jeux
  - Prix de la soumission la plus longue : 94 pages dans les actes et 107 slides
  - Tour de l'horizon de l'évolution de la sécurité des consoles de jeux
    - Playstation 1 : naissance des modchips pour contourner les restrictions de zone
    - Xbox : Chaine de démarrage de confiance, contrôle d'accès au disque dur et signature des binaires
    - Xbox 360 :
      - Erreur d'implémentation dans l'hyperviseur => exploitable avec le jeu King Kong
      - Downgrade la console pour exploiter la vulnérabilité
  - L'ANSSI paye des consoles de jeux ☺

Jour 1

- Rétro-ingénierie matérielle pour les *reversers* logiciels : cas d'un DD externe chiffré par Joffrey Czarny et Raphaël Rigo
  - Etude de l'efficacité d'un disque dur chiffré : Zalman ZM-VE400
    - Le chiffrement est-il robuste ? Correctement implémenté ?
  - Chiffrement indépendant du boitier et basé sur AES-256-XTS
    - Zone réservée à la fin du disque dur
    - Mises à jour du firmware chiffrées
  - La démarche mise en place pour l'étude est bien détaillée



Jour 1

- CLIP : une approche pragmatique pour la conception d'un OS sécurisé par Vincent Strubel
  - Présentation effectuée à la JSSI 2015
  - Isolation de l'OS selon niveaux de sécurité hauts (pour les documents sensibles) et bas (pour les vidéos de chats)
  - Utilisation uniquement pour l'administration et des OIV
  - Pas de partage avec le grand public
- Injection de commandes vocales sur ordiphone par José Lopes Esteves
  - Technique permettant d'envoyer des commandes vocales à l'insu de l'utilisateur
  - Utilisation du câble des écouteurs pour envoyer des commandes
- RowHammer par Nicolas Ruff
  - Explication détaillée des causes de la faille (forcer les changements d'état de transistors)
  - Pas d'explication sur comment passer de « on flip des bits » à « I AM (G)ROOT »
  - http://googleprojectzero.blogspot.fr/2015/03/exploiting-dram-rowhammer-bug-to-gain.html
- FlexTLS : des prototypes à l'exploitation des vulnérabilités dans TLS
  - miTLS bibliothèque cryptographique formellement vérifiée
  - Outil conçu pour tester le protocole et les implémentations existantes
  - Voir la présentation effectuée à l'OSSIR en juin 2015
    - http://www.ossir.org/paris/supports/2015/2015-06-09/p.pdf

Jour 2

Jour 2

- ✓Mon TOP 3
  - ✓VLC, les DRM des Bluray et HADOPI
  - ✓Protocole HbbTV et sécurité : quelques expérimentations
  - ✓A Large-Scale Analysis of the Security of Embedded Firmwares

Jour 2

- SSL/TLS, 3 ans plus tard par Olivier Levillain
  - Revue des vulnérabilités découvertes sur le protocole SSL/TLS et ses implémentations
  - Les développeurs font souvent les mêmes erreurs
  - Les spécifications sont assez permissives
- Les risques d'OpenFlow et SDN par Maxence Tury
  - Rappel de ce qu'est un SDN (séparation des fonctions de routage et de transfert)
  - Etude du protocole OpenFlow et identification de faiblesses
    - Absence de TLS pour les communications
    - Possibilité d'effectuer un déni de service
  - Développement de modules Scapy spécifiques
- Quatre millions d'échange de clés par seconde par Adrien Guinet, Carlos Aguilar, Serge Guelton et Tancrède Lepoint
  - Présentation d'une bibliothèque cryptographique : NFLib
  - Améliore les performances pour le calcul cryptographique des algorithmes de chiffrement asymétrique
  - Intéressant par exemple pour la *Perfect Forward Secrecy*

Jour 2

- VLC, les DRM des Bluray et HADOPI par Jean-Baptiste Kempf
  - L'association est née dans les locaux de Centrale Paris
  - Les étudiants voulaient un réseau Ethernet pour… jouer à Doom !
    - Développement d'un logiciel multimédia pour justifier la nécessité d'élargir les tuyaux
  - Présentation des DRM mis en place sur les DVD et les Bluray
  - Echanges entre VLC et Hadopi pour savoir si le projet n'était pas dans l'illégalité
  - N'hésitez pas à les soutenir !
- Analyse de sécurité de technologies propriétaires SCADA par Alexandre Gazet, Florent Monjalet et Jean-Baptiste Bédrune
  - Etude d'un protocole propriétaire de communication entre un PLC et un système de contrôle
  - Choix d'un protocole récent pour éviter les technos trouées de partout
  - Présentation de la démarche de reverse engineering
    - Analyse des paquets envoyés par le PLC
    - Reverse du client Windows (IHM)
  - Des vulnérabilités ont été identifiées et remontées au constructeur

Jour 2

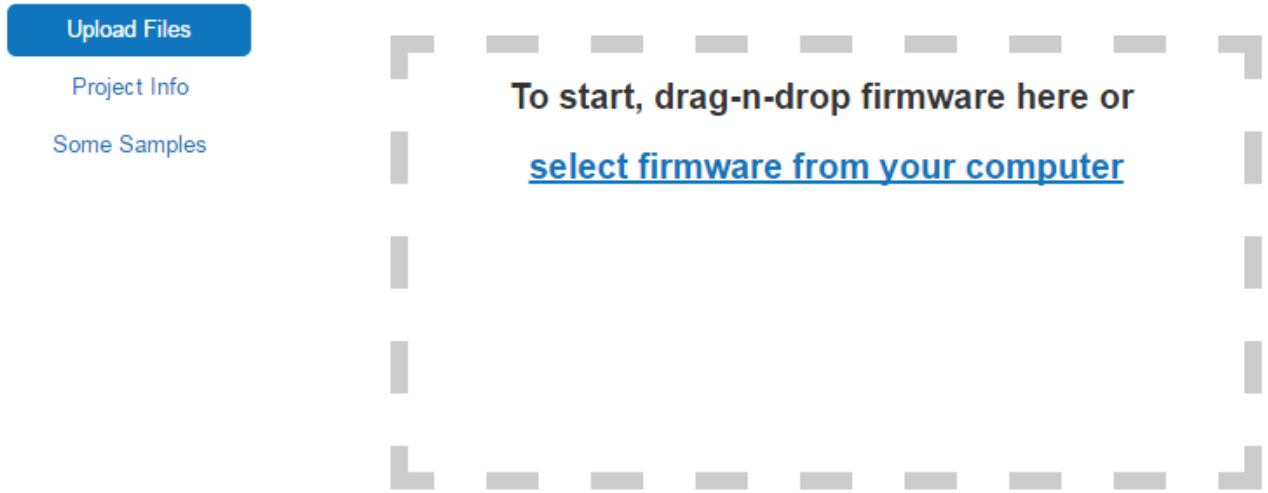
- Protocole HbbTV et sécurité : quelques expérimentations par Eric Alata et al.
  - Aucune authentification du signal reçu par un téléviseur (connecté ou non)
    - Le signal le plus puissant est pris en compte
  - Aucune authentification des données associées à une chaine (TV connectée)
  - Protocole HbbTV permet d'envoyer du contenu Web à une TV
  - Possibilité d'émettre un signal malveillant contenant une URL piégée
    - Inclusion de l'URL dans un « overlay » de la TV (XSS sur IoT, en somme)
    - Payload : envoi de paquets UPnP depuis la TV vers la box pour ouvrir des ports à l'extérieur

Jour 2

- Compromission de carte à puce via la couche protocolaire ISO 7816-3 par Guillaume Vinet
  - Fuzzing sur des cartes puces à partir d'un Arduino, d'un client Python et de l'outil Sully
  - L'auteur envisage d'étendre ses recherches sur les cartes sans contact
- Fuddly : un framework de fuzzing et de manipulation de données par Eric Lacombe
  - Framework de fuzzing et de manipulation de données
  - https://github.com/koretux/fuddly
- Avatar : A Framework to Support Dynamic Security Analysis of Embedded System's Firmwares par Jonas Zaddach
  - Framework Avatar permettant d'effectuer une analyse dynamique de firmwares
  - http://s3.eurecom.fr/tools/avatar/

Jour 2

- A Large-Scale Analysis of the Security of Embedded Firmwares par Andrei Costin
  - Analyse à grande échelle des firmwares des systèmes embarqués
  - Etude de masse sur les vulnérabilités présentes
  - Difficulté pour récupérer des firmwares
  - Analyse effectuée via l'outil BAT (Binary Analysis Toolkit)
  - http://firmware.re – analyse de firmware as a service



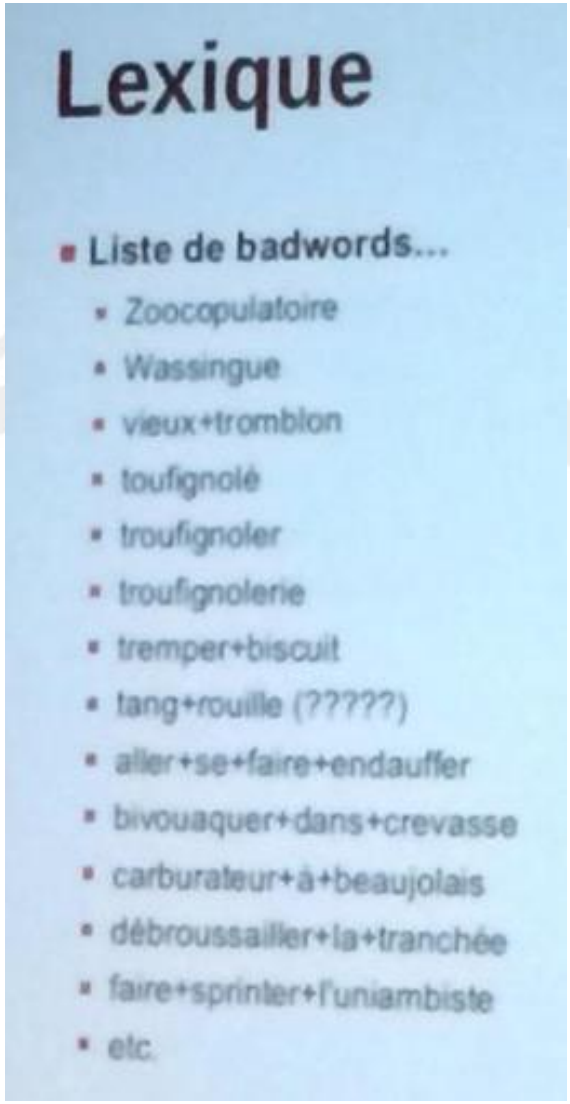
Jour 2

- Résultats du challenge
  - 1498 téléchargements
  - 36 validations
  - 32 solutions détaillées

- Le challenge était décomposé en 3 parties
  1. Partie facile
     - Crypto
     - Analyse de trames USB
     - Forensics
     - Misc
  2. Partie difficile
     - Reverse exotique du ST20
  3. Partie rage
     - Stéganographie récursive

Jour 2

- Rumps
  - Principe : 3min30 pour exposer son sujet
    - Si le public est conquis il se tait, sinon il applaudit ☺
  - Donjons, dragons et sécurité
  - Vulnérabilité sur le site Web de SSTIC
  - $yolo, pour les vrais bonhommes
  - Evasion HQL vers SQL
  - MISC : recherche d'auteurs
  - S(4)u : su pour Windows
  - FIR : le CERT-SocGen recrute
  - Photorec : mieux que EnCase !
  - DFF
    - C'est l'histoire d'un mec qui a perdu son smartphone
  - IVRE, scanner d'Internet
  - Reverse de poupée connectée
  - Annonce de la Botconf à Paris chez Google



Plan

Jour 3

- ✓Mon TOP 4
  - ✓Entre urgence et exhaustivité : de quelles techniques dispose l'analyste pendant l'investigation?
  - ✓Analyse de documents MS Office et macros malveillantes
  - ✓Crack me, I'm famous!: Cracking weak passphrases using freely available sources
  - ✓Snowden, NSA : au secours, les journalistes s'intéressent à la sécurité informatique !

Jour 3

- Utilisation du framework pyCAF pour l'audit de configuration par Maxime Olivier
  - Présentation faisant suite à celle de la JSSI 2013
  - Framework Python permettant d'automatiser l'analyse d'un ensemble de fichiers de configurations (Linux uniquement)
  - Les fichiers doivent être collectés à la main (archive ZIP)
  - github.com/Maximeolivier/pyCAG.git

- Analyse de documents MS Office et macros malveillantes par Philippe Lagadec
  - Les macro reviennent à la mode
  - La réactivation s'effectue en 2 clics
  - Les actions réalisables par une macro sont très larges (déclenchement à l'ouverture, télécharger un fichier, créer un fichier, etc.)
  - Techniques d'obfuscation utilisées par les attaquants pour masquer l'action de la macro
  - Présentation des outils
    - OfficeMalScanner / Officeparser / Oledump / Olevba / ViperMonkey

Jour 3

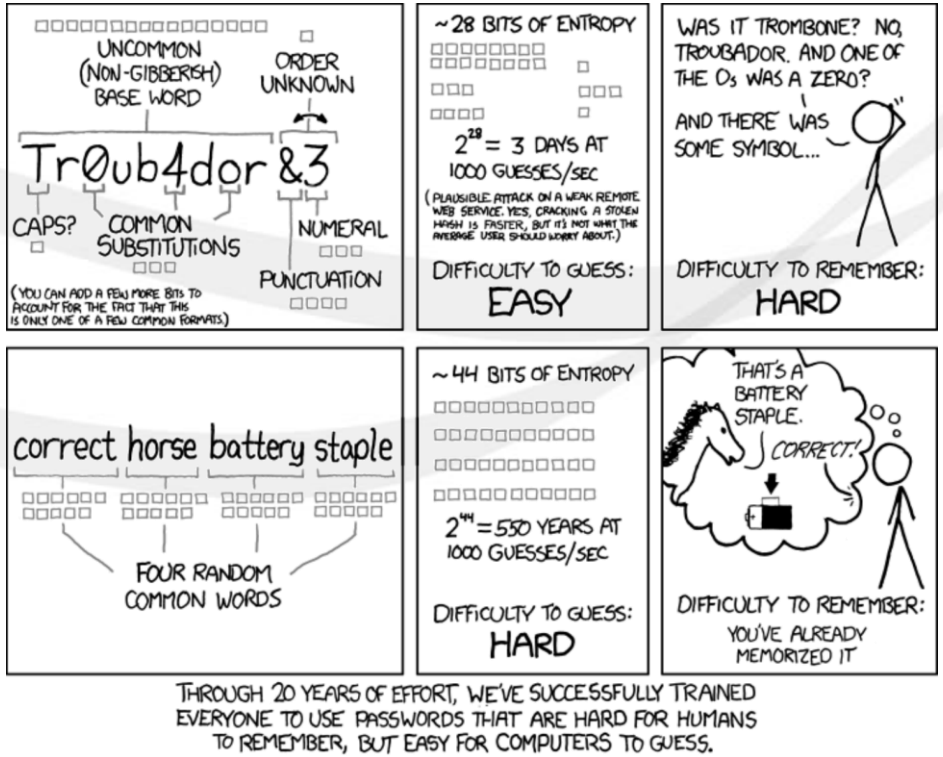
- StemJail : Cloisonnement dynamique d'activités pour la protection des données utilisateur par Mickaël Salaün
  - Il faut protéger les données utilisateur
  - Cloisonnement des processus via l'utilisation de namespaces
  - PoC : https://github.com/stemjail
- Hack yourself defense par Eric Detoisien
  - Un état des lieux du déséquilibre entre attaquants et défenseurs en cyber-sécurité

Jour 3

- Entre urgence et exhaustivité : de quelles techniques dispose l'analyste pendant l'investigation? par Amaury Leroy
  - Retour d'expérience sur la démarche à adopter lors d'une investigation
  - On se concentre uniquement sur les flux réseau et les logs proxy
  - Démarche en 3 étapes
    1. Effectuer des recherches simples et efficaces (marqueurs connus, réduire la quantité d'informations, etc.)
    2. Surveiller l'attaque (détection de navigation automatisée, flux SSL non cohérents, etc.)
    3. Pousser l'analyse en profondeur (visualisation graphique des données pour identifier des tendances)
- IRMA : Incident Response and Malware Analysis par Alexandre Quint, Fernand Lone Sang et Guillaume Dedrie
  - Plateforme modulaire permettant d'effectuer l'analyse d'un fichier ou d'un binaire inconnu
  - Eviter l'envoi de documents sur un service en ligne (VirusTotal)
  - Actuellement 20 antivirus supportés
  - Interroge virustotal uniquement sur le condensat du fichier analysé
  - Extraction de métadonnées
  - La communauté doit s'agrandir sur ce projet

Jour 3

- Crack me, I'm famous!: Cracking weak passphrases using freely available sources par Hugo Labrande
  - Comment casser des phrases de passe longues
  - Collecte de phrases sur Wikipedia, commentaires Youtube, WikiQuotes, RapDict, etc.
  - Constitution d'un dictionnaire de 65 millions de candidats
  - Utilisation de JTR sur un PC personnel pour casser des mots de passe



Ce genre de construction ne fonctionne pas si la phrase est célèbre…

Jour 3

- CSinmactaiat. : « Computer science is no more about computers than astronomy is about telescopes. » - Dijikstra.
- mvpumelvqlveum : « Más vale perder un minuto en la vida que la vida en un minuto » - proverbe espagnol.
- tbtitbtwtbtewb : « The best there is, the best there was, the best there ever will be » - Bret "The Hitman" Hart.
- wowowhiyhaynwa : « Walk on, walk on, with hope in your heart And you'll never walk alone » - fans du Liverpool FC.
- uuddlrlrababsS : « Up Up Down Down Left Right Left Right A B A B select Start » - Konami Code
- tamtihaehtadoiyp : « There are more things in heaven and earth, Horatio, than are dreamt of in your philosophy. » - Hamlet.
- 1lomtjjzictcttsdkcs (19 char) : « Litwo ! Ojczyzno moja ! ty jestes jak zdrowie ; Ile cie trzeba cenic, ten tylko sie dowie, Kto cie stracil... » - ouverture de Pan Tadeusz, poème épique polonais.

Jour 3

- Contextualised and actionable information sharing within the cyber-security community par Frédéric Garnier
  - Présentation d'un modèle de threat intelligence et partages d'informations
- Snowden, NSA : au secours, les journalistes s'intéressent à la sécurité informatique ! par Martin Untersinger
  - Martin est journaliste au journal Le Monde
  - Qu'a-t-on appris 2 ans après les révélations de Snowden ?
  - La NSA collecte tout, mais il apparait qu'aucun acte terroriste n'a pu être arrêté via ce dispositif
  - Néanmoins la France suit le même chemin avec la Loi Renseignement
  - 30 % des américains changent leurs habitudes

Jour 3

- Les journalistes ne sont pas très compétents en sécurité

- Mais, il faut vulgariser pour être compris
- Ceux qui parlent aux journalistes veulent vendre quelque chose
- Appel aux experts de sécurité afin d'établir un dialogue avec les journalistes et sensibiliser le grand public

Conclusion

- Très bonne conférence comme toujours ☺
- Conférences variées et accessibles
- Il a fait beau pendant 3 jours !!!
- 1/3 de l'assemblée venait pour la première fois
- Un social event toujours aussi social !
- La retransmission en streaming était top !
- Et toujours du troll !!!!

Conclusion

- D'autres résumés sont disponibles
  - Blog XMCO
    - http://blog.xmco.fr/index.php?post/2015/06/17/Retour-sur-%C3%A9dition-2015-SSTIC
  - Podcast No Limit Secu
    - http://www.nolimitsecu.fr/sstic-2015/
  - Liveblogging de nosecure
    - http://www.nosecure.org/
  - Intrinsec
    - http://securite.intrinsec.com/2015/06/23/sstic-2015-premiere-journee/
    - http://securite.intrinsec.com/2015/06/23/sstic-2015-deuxieme-journee/
    - http://securite.intrinsec.com/2015/06/23/sstic-2015-troisieme-journee/
- Les actes, présentations et vidéos sur le site du SSTIC
  - https://www.sstic.org/2015/actes/

Merci de votre attention

Questions ?

Site Intrinsec
www.intrinsec.com

Blog Intrinsec Sécurité
securite.intrinsec.com

Twitter Intrinsec
@Intrinsec_Secu