intrinsec
BUSINESS CONTINUITY AND SECURITY

Compte-rendu SSTIC 2013

5, 6 et 7 juin 2013

OSSIR Paris / 11 juin 2013

Guillaume Lopes – Consultant Sécurité
Guillaume.Lopes@Intrinsec.com

- Conférence de sécurité à Rennes
- 11ème édition
- Programme
  - → https://www.sstic.org/2013/programme/

Jour 1

- Mon TOP 3

1. Polyglottes binaires et implications
2. Innovation en crypto symétrique
3. (L')Embarqué entre Confiance et Défiance

Innovation en crypto symétrique par Joan Daemen

- http://en.wikipedia.org/wiki/Joan_Daemen
- Rappels de la cryptographie depuis DES jusqu'à aujourd'hui
- Focus sur AES et SHA-3
- En conclusion
  - ✓ Essayer plusieurs idées
  - ✓ Garder les bonnes idées ☺
  - ✓ Equipe avec des compétences complémentaires
  - ✓ Pas trop d'égo dans l'équipe
- Slides
  - ✓ https://www.sstic.org/media/SSTIC2013/SSTIC-actes/conf_ouverture_2013/SSTIC2013-Slides-conf_ouverture_2013-daemen.pdf

- **Mise à plat de graphes de flot de contrôle et exécution symbolique par Eloi Vanderbéken**
  - Techniques de débrouillage de code pour simplifier le reverse
    - ✓ Suivi d'exécution
    - ✓ Suivi de données
    - ✓ Analyse statique
  - Simplifier le graphe d'exécution
  - Outil qui marchouille et « présentation d'escroc » (dixit l'auteur)
  - Sans doute une release pour bientôt

Polyglottes binaires et implications par Ange Albertini

- Fichier polyglotte == Fichier pouvant être interprété de différences façons
  - ✓ Exemple : GIFAR
- Formats étudiés : PE / HTML / PDF / ZIP
- Permet de contourner les antivirus / Faciliter les exfiltrations
- Quelques plantages des différents parseurs ont été réalisés !
- Conclusion => La confusion de type c'est le mal
- Slides : http://fr.slideshare.net/ange4771/polyglottes-binaires-et-implications

- **Recompilation dynamique de codes binaires hostiles par Sébastien Josse**
  - Difficulté à analyser les malwares (statique ou dynamique)
  - Peu d'outils conventionnels disponibles
  - Présentation d'un outil de désobfuscation de malware
    - ✓ Spécifique aux malwares
    - ✓ Automatisation des tâches fastidieuses et répétitives
  - Un shareware sera sans doute mis à disposition
  - Mention spéciale sur la qualité des images du support ☺

Présentation courtes

- Parsifal un parseur robuste réalisé en Ocaml par Olivier Levillain
  - ✓ Parseur de formats binaires
  - ✓ Code : https://github.com/ANSSI-FR/parsifal
  - ✓ Slides : https://www.sstic.org/media/SSTIC2013/SSTIC-actes/parsifal/SSTIC2013-Slides-parsifal-levillain.pdf

* mais ne protège pas des XSS

- Nftables par Eric Leblond
  - ✓ Plus performant par rapport à Netfilter
  - ✓ Simplification de la syntaxe
  - ✓ Slides : https://www.sstic.org/media/SSTIC2013/SSTIC-actes/nftable/SSTIC2013-Slides-nftable-leblond.pdf
  - ✓ HOWTO : https://home.regit.org/netfilter-en/nftables-quick-howto/

- **Compromission d'un terminal sécurisé via l'interface carte à puce par Guillaume Vinet**
  - Création d'un émulateur physique de carte à puce à base d'Arduino
  - Buffer Overflow permettant de dumper le code applicatif du terminal sur son propre écran
  - Dump de la RAM du terminal (uniquement la dernière transaction)
    - ✓ Dans certains cas, le code PIN était présent

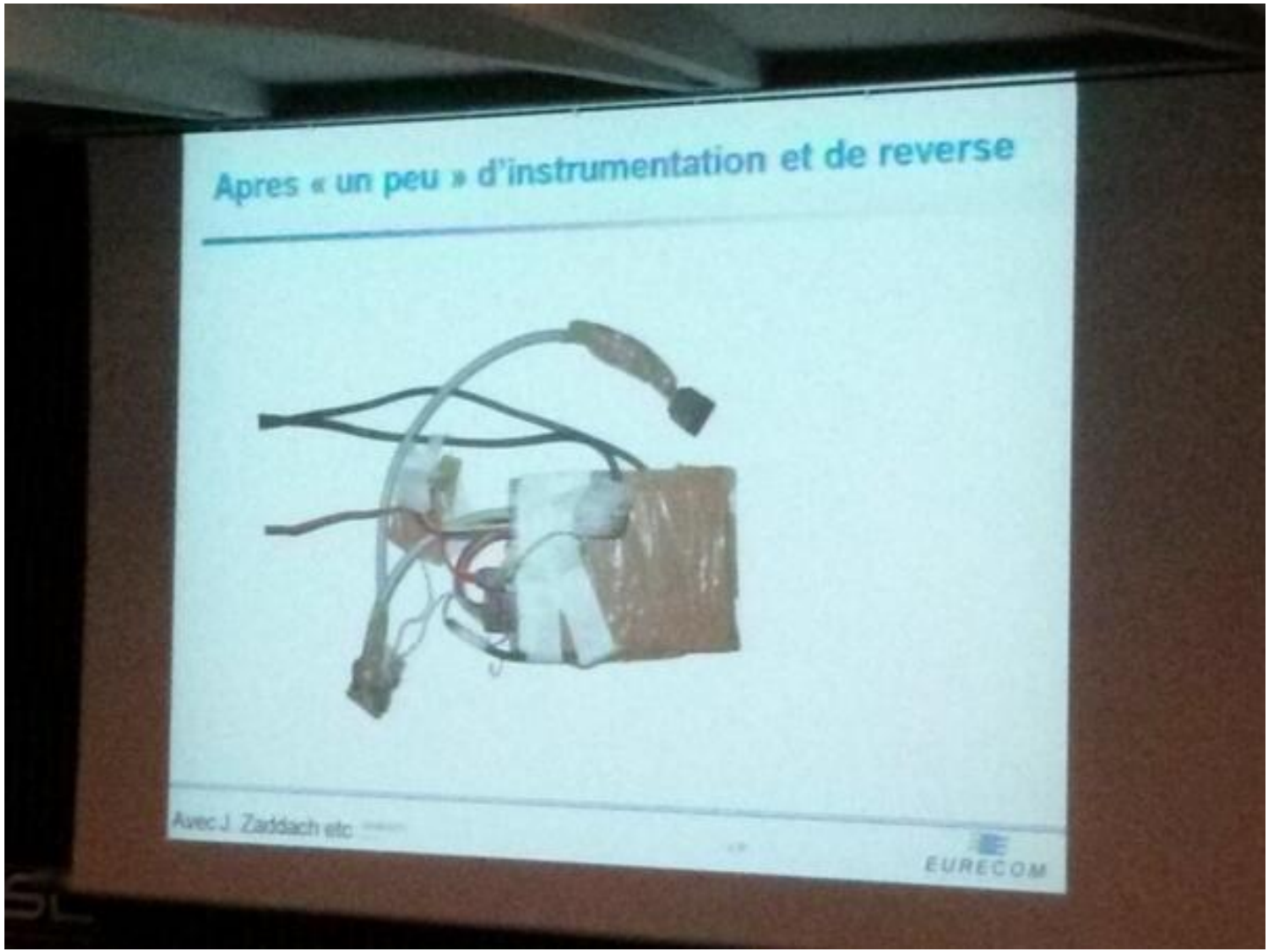
Eric FREYSSINET @ericfreyss 5 Juin
Dump du code via le LCD ... faut filmer et passer par OCR ? #SSTIC
Ouvrir

- **Attaques applicatives via périphériques USB modifiés infection virale et fuites d'informations par Benoit Badrigans**
  - Les clés USB deviennent un fléau
    - ✓ Boucher les ports USB avec du béton ou utiliser des cadenas !!
  - Exfiltration de données
    - ✓ Possibilité d'écrire sur une clé USB montée en lecture seule
  - Contournement des antivirus
  - Slides
    - ✓ https://www.sstic.org/media/SSTIC2013/SSTIC-actes/Attaques_applicatives_via_peripheriques_USB_modifi/SSTIC2013-Slides-Attaques_applicatives_via_peripheriques_USB_modifies_infection_virale_et_fuites_d_informations-badrignans.pdf

Red October par Nicolas Brulez

- Campagne depuis 2007
- Aucun exploit 0-day utilisé
  - ✓ Exploitation classique par spear phishing et fichier Word ou Excel vérolé
- Plus de 300 entités infectées dont 4 en France
  - ✓ http://www.securelist.com/en/images/vlill/kaspersky_lab_infographic_red_october_victims_by_country.png
- Le NDD le plus utilisé avait été mal orthographié par les attaquants
  - ✓ Kaspersky l'a donc enregistré à des fins statistiques
- Démo FAIL !

- **(L')Embarqué entre Confiance et Défiance par Aurélien Francillon**
  - Problématique : Peut-on faire confiance aux systèmes embarqués ?
  - Exemples de failles ?
    - ✓ Baseband HTC G1 : Boot signé par certificat
      - 2 types de certificat commercial et gouvernemental => Pourquoi ?
    - ✓ Disques dur : Possibilité de réécrire le firmware du disque
    - ✓ Voiture sans contact : Attaque par relais avec un câble !!
    - ✓ Protocole ADS-B : Absence de sécurité
  - Présentation sponsorisée par SCOTCH


Apres « un peu » d'instrumentation et de reverse
Avec J. Zaddach etc
EURECOM

Jour 2

- Mon TOP 3

1. Compromission d'un environnement VoIP Cisco
2. Sécurité des applications Android constructeurs et backdoors sans permission
3. UEFI et bootkis PCI : Le danger vient d'en bas

- **Dreamboot et UEFI par Sébastien Kaczmarek**
  - Présentation d'UEFI : Presqu'un vrai OS
    - ✓ Suppression des limites du BIOS, multi-architectures, développé en C
  - Présentation du bootkit Dreamboot
  - Outil : https://github.com/quarkslab/dreamboot

- **UEFI et bootkis PCI : Le danger vient d'en bas par Pierre Chifflier**
  - Présentation axée sur les cartes graphiques
  - Plus de détails dans les actes
- Slides
  - https://www.sstic.org/media/SSTIC2013/SSTIC-actes/uefi_et_bootkits_pci/SSTIC2013-Slides-uefi_et_bootkits_pci-chifflier.pdf

- **Programmation d'un noyau sécurisé en Ada par Arnauld Michelizza**
  - Pourquoi les OS actuels sont de plus en plus vulnérables ?
    - ✓ Complexité, bogues, omniprésents et connectés en permanence
  - Adoption des contre-mesures
    - ✓ Bit NX, ASLR, Segmentation, Pagination, Canaris, etc.
  - Prouver 8500 lignes de C => 200 000 lignes de preuve
    - ✓ 11 ans homme de travail
  - Programmer un noyau en ADA
    - ✓ Absence de buffer overflows, integer overflows et déférencement de pointeurs nuls
  - Slides
    - ✓ https://www.sstic.org/media/SSTIC2013/SSTIC-actes/programmation_d_un_noyau_securise_en_ada/SSTIC2013-Slides-programmation_d_un_noyau_securise_en_ada-michelizza.pdf

- **Ou sinon il existe un autre moyen de faire un noyau sécurisé**

- **Présentation de la solution du challenge SSTIC 2013 par Emilien Girault**
  - Canaux cachés, FPGA, PostScript et vCard
  - Solution
    - ✓ http://static.sstic.org/challenge2013/egirault.pdf

- **La couleur du Net par Laurent Chemla**
  - Filtrage et neutralité du net
  - Présentation avec le plus de chatons ☺
  - En conclusion il faut lire The Shockwave Rider de John Brunner

Présentations courtes

- Vulnérabilité Android Samsung par Etienne Comet
  - ✓ Encore des failles liées aux surcouches des constructeurs
  - ✓ C'était mieux avant avec son nokia 3310
- Compromission d'un environnement VoIP Cisco par @Francisco
  - ✓ Prise de contrôle d'un Cisco Unified Call Manager
  - ✓ Vulnérabilités classiques : injection SQl, exécution de commandes, élévation de privilèges, etc.
  - ✓ N.B : Cisco n'a pas été contacté par l'orateur ☺
- Observatoire de la résilience de l'Internet français par Guillaume Valadon
  - ✓ Passage en revue de problématiques BGP et des AS
  - ✓ https://www.sstic.org/media/SSTIC2013/SSTIC-actes/resilience_internet/SSTIC2013-Slides-resilience_internet-valadon.pdf

- **Sécurité des applications Android constructeurs et backdoors sans permission par André Moulu**
  - Axé sur la Samsung Galaxy S3
  - Système de permission défaillant
    - ✓ Accès à la carte SD, envoi de SMS, accès à Internet
  - Création d'une suite d'outils nommée ASA (pas encore disponible)
  - Les failles ont été remontées à Samsung

- **Limites des tables Rainbow et comment les dépasser en utilisant des méthodes probabilistes optimisées**
  - Rien de vraiment nouveau / Manque de stats précises

- **Rump sessions** (3 min 30 par rump / Plus de 20 rump)
  1. Divers SSTIC
     - ✓ Il faut soumettre !! (minimum 7 pages)
     - ✓ Vagues d'inscription au SSTIC rapides
       - Environ 10 minutes par vague sauf la dernière 50 minutes
     - ✓ Encore beaucoup de nouveaux cette année (1/3 à la louche)
  2. MGCP : Un protocole VoIP oublié par Joffrey Czarny
  3. Quel est l'OS de Kim Jong-Un par Pierre Capillon
     - ✓ http://java-0day.com (Réponse MacOS)
  4. La sécurité est un échec par Nicolas Ruff
     - ✓ Présentation de vulnérabilités sur UCO_IA
  5. Another Perspective to IP-Darkspace Analysis
  6. L'histoire d'un bug vieux de 20 ans
     - ✓ Vulnérabilité PATHALLOC (cf. NoSuchCon??)

Rump sessions

7. Cloud ISO 14001 par Arnaud Ebalard
   - ✓ Installation d'un cloud privé à la maison
   - ✓ NETGEAR ReadyNAS 102
8. WTF avec Suricata par Eric Leblond
9. Rappels sur d'autres conférences (PUB)
   - ✓ Botconf à Nantes les 5 et 6 décembre 2013
   - ✓ GreHack à Grenoble le 15 novembre
   - ✓ OWASP EU Tour à Sophia Antipolis le 24 juin
10. Raspberry Spy par Antoine Cervoise
11. ME@YOUR.HOME => Cambriolage 2.0
12. IOC par Ivan Fontarensky
13. Programmation noyau sécurisé ADA => Démo

Rump sessions

14. Stack overflow et Stack-based buffer overflow
15. Analyse d'AD par Philippe Biondi
    - ✓ Outil python permettant d'extraire les données du fichier ntds.dit
    - ✓ Import dans une base de données MongoDB
16. Panda OCR par Panda
17. Hack my CCTP par Anonymous
18. RW2 Des photos... sans photorec par Raphael rigo
19. Récupération de données Photorec par Christophe Grenier
    - ✓ Qphotorec (outil graphique)
20. Je choisis l'option offensive ! par Florent Chabaud
21. TNS bit flip attack par Nicolas Collignon
    - ✓ MITM sur TNS Oracle
    - ✓ Houracle => proxy tns

Jour 3

- Mon TOP 3

1. Fuzzing intelligent de XSS type-2 Filtrés selon Darwin : KameleonFuzz
2. La réponse aux incidents ou quelques recommandations
3. Faire face aux cybermenaces => Détecter les attaques et former des experts en SSI

- **Fuzzing intelligent de XSS type-2 Filtrés selon Darwin : KameleonFuzz par Fabien Duchêne**
  - Fuzzing = Frelatage en français
  - Outil KameleonFuzz (python)
  - Inférence de modèle + fuzzing évolutionnaire

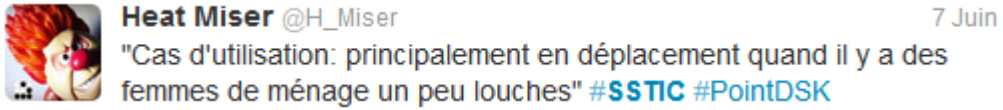
- **Fingerprinting de navigateurs par Erwan Abgrall**
  - Identifier le bon exploit pour le bon navigateur
  - Fingerprinting à base de XSS
  - Distance de Hamming
  - Slides : http://xss.labosecu.rennes.telecom-bretagne.eu/static/prez/fingerprinting.html#1
  - Outils : http://xss.labosecu.rennes.telecom-bretagne.eu/

- **Duqu contre duqu : rétroconception du driver par Aurélien Thierry**
  - Décompilation du driver de Duqu
  - Création d'un driver défensif pour détecter Duqu
- **Le TEE, nouvelle ligne de défense dans les mobiles par Hervé Sibert**
  - Trusted Executed Environnment
  - Déporté les fonctionnalités sensibles
- **La réponse aux incidents ou quelques recommandations par Alexandre Dulaunoy**
  - Bonnes pratiques pour l'écriture d'un malware
  - MiniDuke est un bon malware
  - Voir le guide OPSEC

Heat Miser @H_Miser 7 Juin
"Les IDS détectent les événements, mais comme personne ne lit les logs... " #SSTIC
Ouvrir

Présentations courtes

- Détection comportementale de malware P2P par analyse réseau par Xiao Han
  - ✓ http://fr.wikipedia.org/wiki/Machine_%C3%A0_vecteurs_de_support
- Attestation distante d'intégrité sous Android par Dimitri Kirchner
  - ✓ Attester l'intégrité d'un poste de travail via son téléphone Android
  - ✓ Outil Android-attest (pas encore disponible)



- Le rôle des hébergeurs dans la détection de sites Web compromis par Davide Canali
  - ✓ Testé les hébergements mutualisés en les compromettant intentionnellement et attendre la réaction de l'hébergeur
  - ✓ Un seul hébergeur a détecté une compromission mais n'a pas prévenu le client

- **Conférence de clôture : Faire face aux cybermenaces => Détecter les attaques et former des experts en SSI par Ludovic Mé**
  - « Y que les vieux cons qui font les conférences de clôture »
  - Passage en revue des objectifs du livre blanc 2013
  - Première partie sur la détection d'intrusions
    - ✓ Il faut diminuer le taux de faux positifs
    - ✓ La détection d'intrusion est un échec !
  - Seconde partie sur la formation
    - ✓ Former plus tôt
    - ✓ Former les formateurs
    - ✓ Il faut former les gens à l'offensif !
    - ✓ Besoin de gens compétents
    - ✓ Cyber Réserve

Conclusion

Conclusion

- Très bonne conférence
  - Toujours du troll !
  - Des 0-days
- Niveau homogène des conférences
  - Hormis la conférence d'ouverture sur la crypto
- Plus de présentations courtes par rapport à l'édition précédente
- Conférence toujours aussi conviviale
- Toujours autant de nouveaux et de vieux piliers
- Il a fait beau pendant 3 jours !!
- La DGA recrute !

Conclusion

- Comptes rendus en ligne
  - securite.intrinsec.com/tag/sstic/
  - http://www.n0secure.org/
  - http://www.devoteamblog.com
  - http://www.mdal.fr/
  - http://quack1.me
  - http://www.sebnet.org/article/sstic-edition-2013/
- Vidéos en ligne des rumps
  - http://www.dailymotion.com/user/Vengeur_Masqu/1

intrinsec
BUSINESS CONTINUITY AND SECURITY

Merci de votre attention
Questions ?