

24



ETHICALHACKINGCONTEST

INSOMNI'HACK

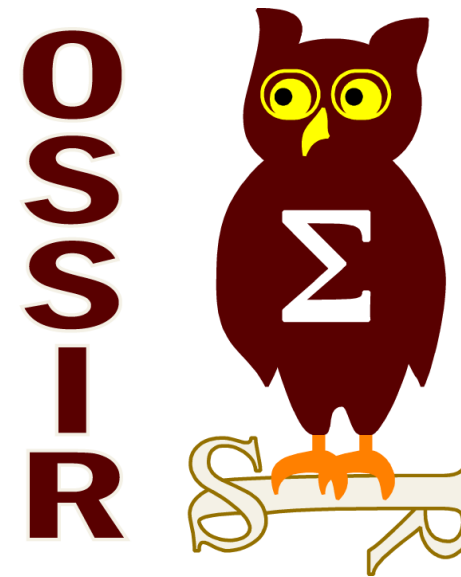
Compte-rendu Insomni'hack 2016



- OSSIR Paris : 12 avril 2016

Walid Arnoult
Consultant Sécurité
Walid.Arnoult@intrinsec.com
+33 1 41 91 58 87

Arthur Villeneuve
Consultant Sécurité
Arthur.Villeneuve@intrinsec.com
+33 1 41 91 58 82



Info

- 9^{ème} édition
- Conférence de sécurité organisée par la société SCRT
- Du 17 au 19 mars 2016
 - Workshops (le 17)
 - Analyse forensic de systèmes Windows avec des outils gratuits (Sébastien Andrivet)
 - Sécurité des applications Web avancées (Alain Mowat)
 - Utilisation avancée de Metasploit (Adrien Stoffel & Julien Oberson)
 - Conférence (le 18)
 - CTF (le 18 de 18h à 4h)



04:30:00

REVEIL



07:15:00

Vol Paris - Genève

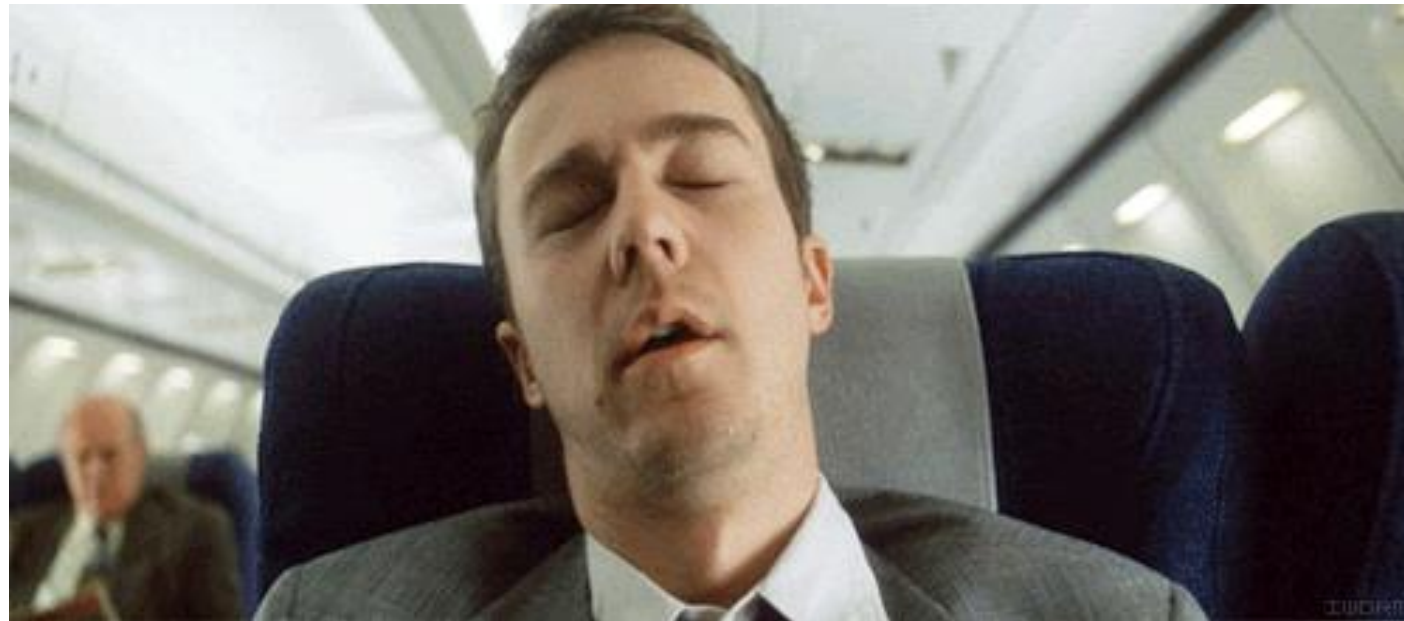
PARIS

CDG



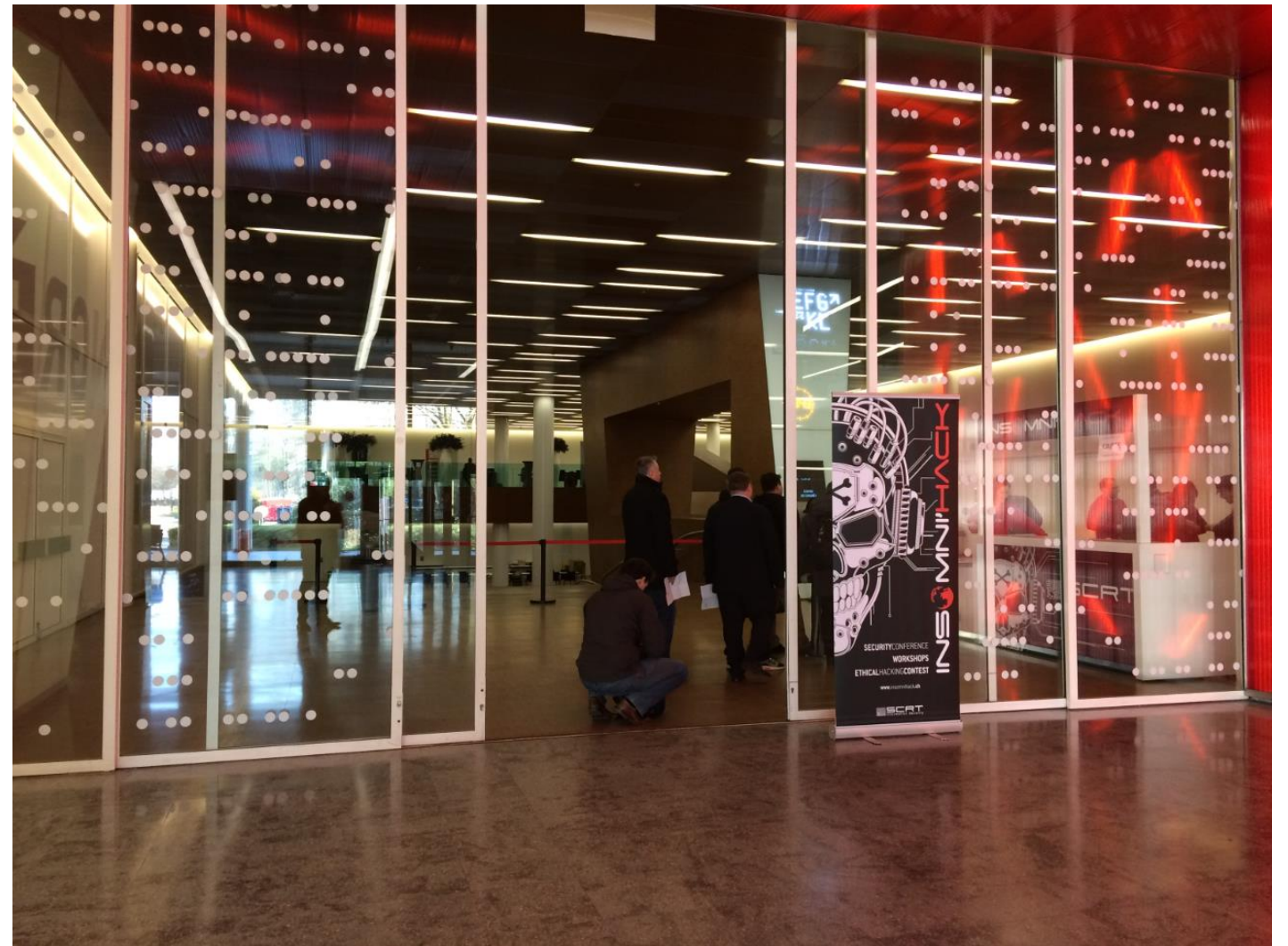
GENÈVE

GVA



08:30:00

Arrivée au Palexpo



09:00:00

Petit tour des stands



09:30:00

Début des conférences

Time	Track 1 (room K)	Track 2 (room F)	Track 3 (room G)
9h30 - 10h15	A Hippocratic Oath for Connected Medical Devices Beau Woods	Crypto code: the 9 circles of testing JP Aumasson	–
10h15 - 10h45		Coffee break	
10h45 - 11h30	IAEA – The role of the IT security specialists at the International Atomic Energy Agency. Massimiliano Falcinelli	Unboxing the White-Box Eloi Sanfelix	Criminal Hideouts for Lease: Bulletproof Hosting Services Maxim Goncharov
11h45 - 12h30	Million Dollar Baby: An “angr”y Attempt at Conquering the DARPA CGC Nick Stephens	Building Trust by Design Hoang Bao	8 security lessons from 8bit games Florian Hammers
12h30 - 14h00		LUNCH	
14h00 - 14h45	Beating the trust out of the root of trust Frederic Jacobs	Cyber criminalité, recrutement djihadiste : “le facteur humain” dans les affaires cyber Frank Decloquement	Reversing Internet of Things from mobile applications Axelle Aprville
15h00 - 15h45	DDoS Surviving or mitigating René Luria	4G/LTE Security : l’état de l’art Sylvain Maret	Lessons learnt from the history of vulnerabilities in hypervisors Rafal Wojtczuk
15h45 - 16h00		Coffee break	
16h15 - 17h	From Bored Hacker to Board CISO, a short-n-fun tale Bruno Kerouanton		

09:30:00

Conférence - A Hippocratic Oath for Connected Medical Devices



Beau Woods

@beauwoods

Globe-Trotting Infosec Veteran •
Reformed technologist • Doing what I
love; loving what I do

beauwoods.com

Inscrit en avril 2007

Conférence - A Hippocratic Oath for Connected Medical Devices

- 10 ans d'expérience dans le milieu médical
- @iamthecavalry



- 5 questions posées aux parties prenantes du milieu de la santé :
 - Qui êtes-vous ?
 - Quels sont vos espoirs ?
 - Quelles sont vos peurs ?
 - Si vous aviez une question à poser, quelle serait-elle ?
 - Qu'est-ce que vous pouvez apporter ?

Conférence - A Hippocratic Oath for Connected Medical Devices

- Serment basé sur 5 composants :
 - Conception sécurisée des produits
 - Collaboration des tiers
 - Divulgation de bugs
 - Extraction de preuve
 - Améliorer les investigations
 - Résilience et confinement
 - Sous-marin
 - Mises à jour de cyber[®] sécurité

- Appel à l'action afin de :
 - Préconiser
 - Adopter
 - Adapter
 - Enrichir
 - Collaborer

Conférence - Crypto code: the 9 circles of testing



JP Aumasson
@veorq

cryptosecurity — 131002.net/siphash —
blake2.net — cryptocoding.net —
password-hashing.net — norx.io

📍 Switzerland
🔗 aumasson.jp
📅 Inscrit en juin 2009

Conférence - Crypto code: the 9 circles of testing

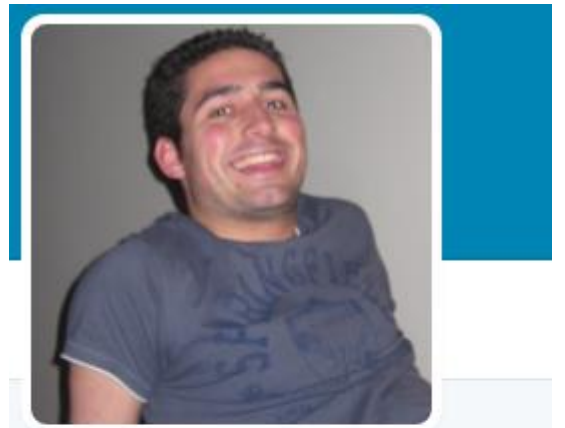
- La plupart des problèmes de cryptographie récents auraient pu être évités à l'aide de 9 axes de test
- Vecteurs de test
 - Faire des tests unitaires sur toutes les fonctionnalités
- Les bugs simples
 - Buffer overflow, corruption de mémoire, fuites d'information
 - Faire des analyses statiques du code et du fuzzing
- Mauvaise utilisation du logiciel
 - Bien gérer les mauvaises entrées utilisateurs et gérer correctement les erreurs
- Les fonctionnalités optionnelles
 - Présence de fonctionnalités optionnelles qui ne sont pas testées et comportent des vulnérabilités

Conférence - Crypto code: the 9 circles of testing

- Génération de nombres aléatoires
 - Faire des tests statistiques sur les aléas
- Timing leak
 - Le temps d'exécution doit être constant et non dépendant de la taille de la clé ou des fonctions utilisées
- Le fuzzing
- Les preuves mathématiques
 - Est-ce que ma fonction de chiffrement est mathématiquement prouvée ?
- Les tests physiques
 - Side channel, résistance aux fautes

10:45:00

Conférence - Unboxing the White-Box



Eloi Sanfelix

@esanfelix

Security analyst, challenging security of embedded hardware and software, mostly for the payment and content protection industries. #int3pids CTF player.

📍 NL

🔗 limited-entropy.com

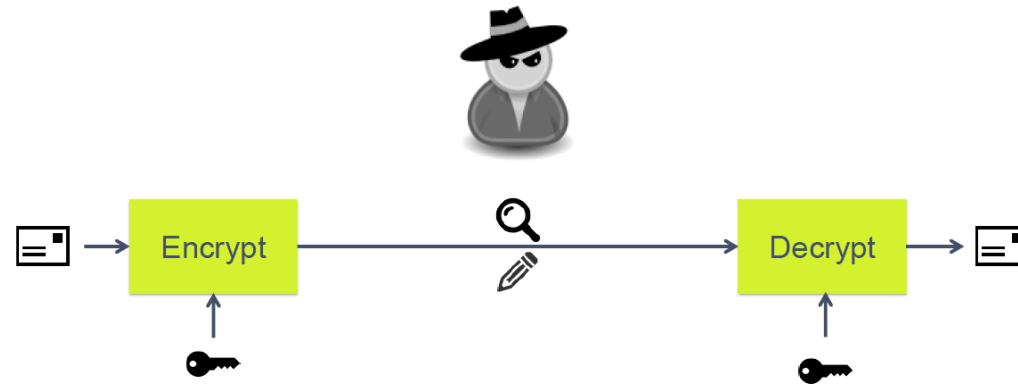
📅 Inscrit en septembre 2009

Conférence - Unboxing the White-Box

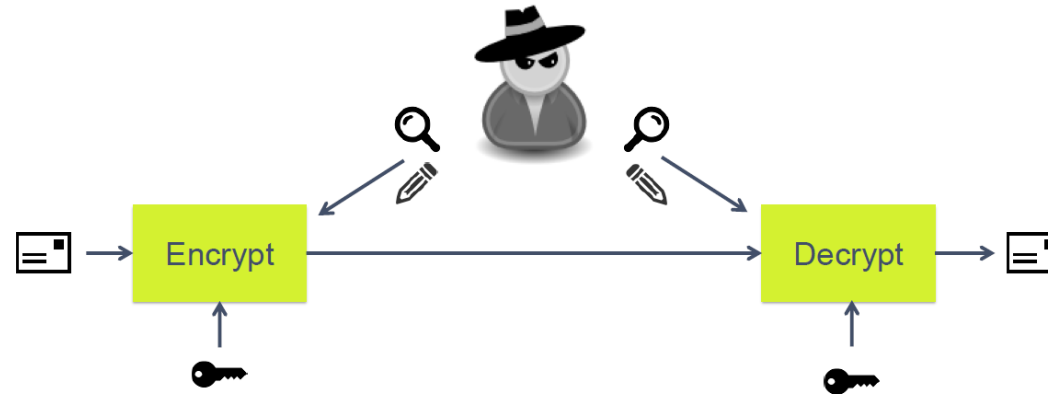
- Cryptographie White-Box
 - Protéger contre l'extraction de clé
- Utilisation
 - Application de paiement mobile
 - Protection des contenus
 - Cryptographie dans le cloud
- Attaque White-box
 - Man-At-The-End
 - Récupérer les clés de chiffrement

Conférence - Unboxing the White-Box

- Black-Box



- Gray-Box



- White-box

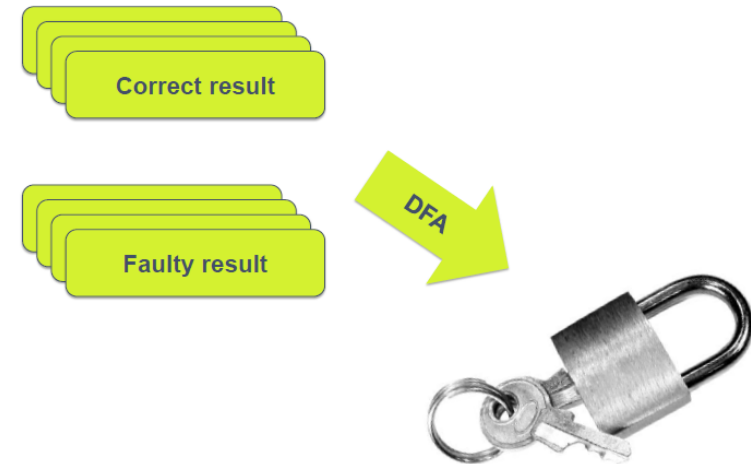


Conférence - Unboxing the White-Box

- Attaques :

- Differential Fault Analysis (DFA)

1. Localisation d'un point d'injection
2. Récupération des échantillons
3. Analyse des erreurs générées



- Side channel Analysis (SCA)

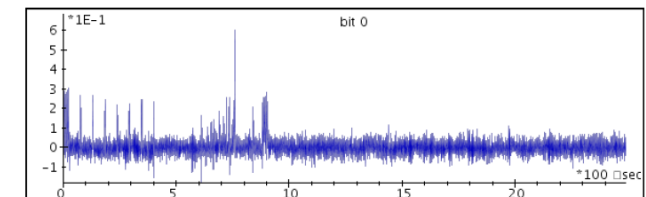
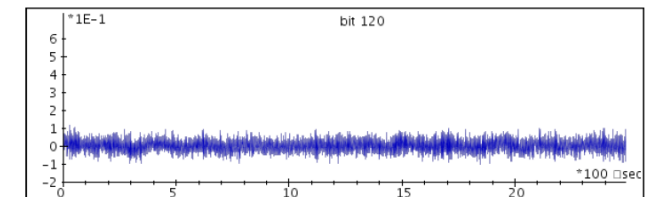
1. Instrumentation

- Instrumentation (PIN, Valgrind)
- Instantané de la pile par tour (Hooking, debugger)
- Emulation (QEMU, Unicorn, PANDA)

2. Exécution multiple de données aléatoires

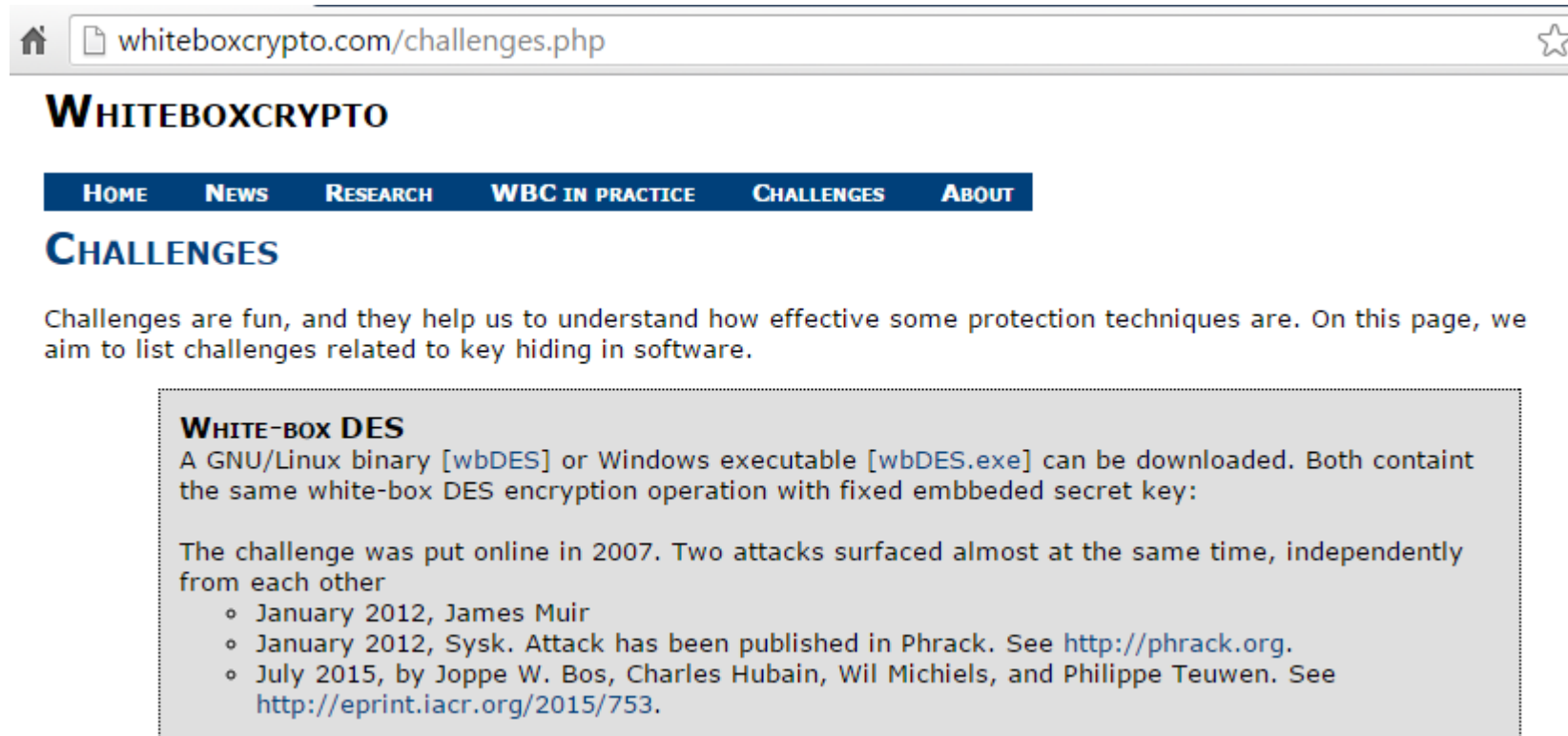
3. Récupération des données de mesure

4. Analyse SCA



Conférence - Unboxing the White-Box

- Démo :
 - Challenge wbDES



whiteboxcrypto.com/challenges.php

WHITEBOXCRYPTO

HOME NEWS RESEARCH WBC IN PRACTICE CHALLENGES ABOUT

CHALLENGES

Challenges are fun, and they help us to understand how effective some protection techniques are. On this page, we aim to list challenges related to key hiding in software.

WHITE-BOX DES
A GNU/Linux binary [wbDES] or Windows executable [wbDES.exe] can be downloaded. Both contain the same white-box DES encryption operation with fixed embedded secret key:

The challenge was put online in 2007. Two attacks surfaced almost at the same time, independently from each other

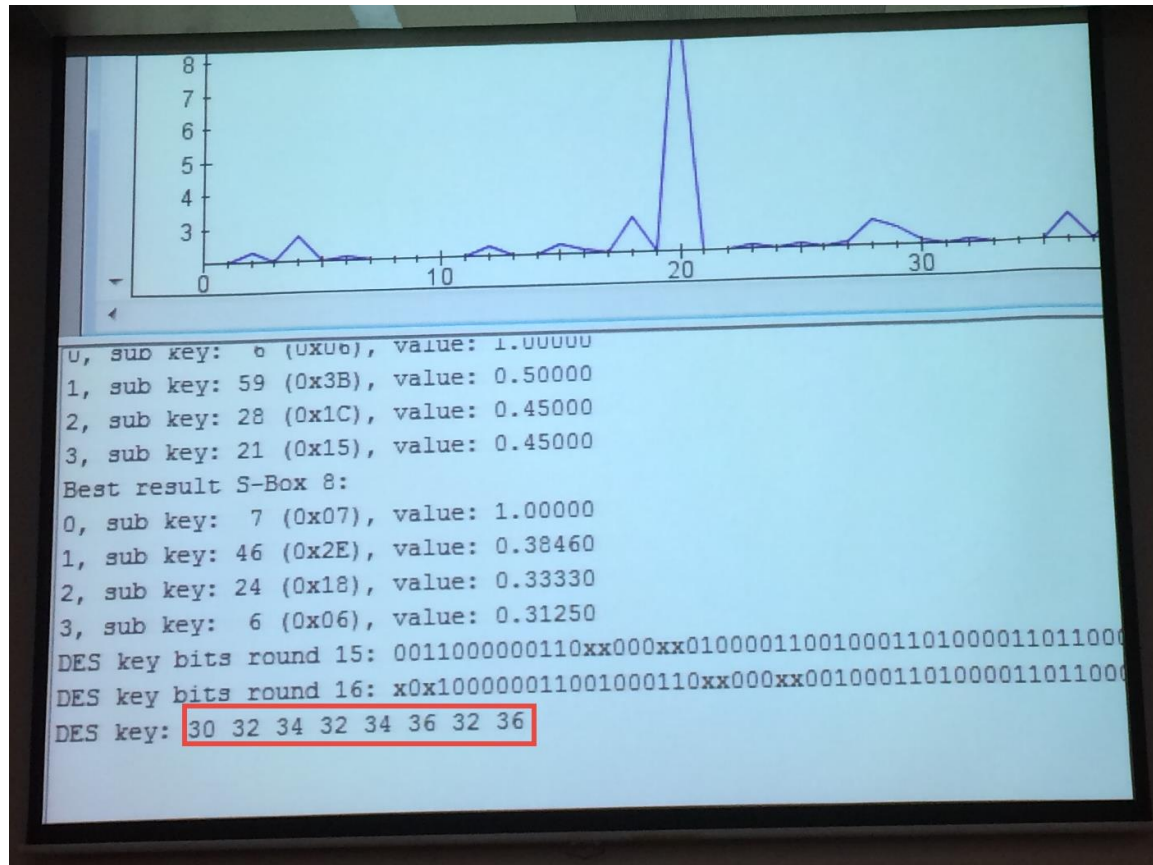
- January 2012, James Muir
- January 2012, Sysk. Attack has been published in Phrack. See <http://phrack.org>.
- July 2015, by Joppe W. Bos, Charles Hubain, Wil Michiels, and Philippe Teuwen. See <http://eprint.iacr.org/2015/753>.

- Clé de chiffrement DES cachée : 0x30 0x32 0x34 0x32 0x34 0x36 0x32 0x36

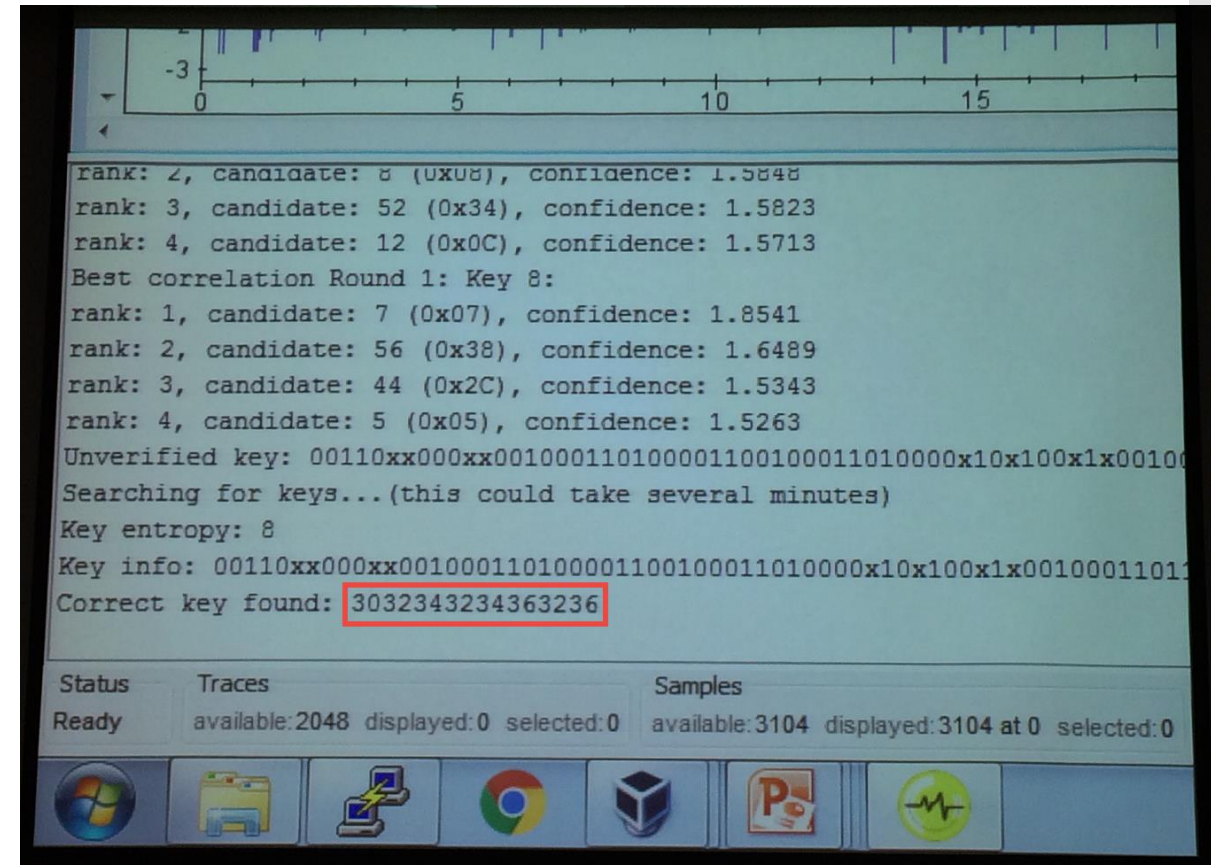
Conférence - Unboxing the White-Box

- Récupération de la clé de chiffrement DES

- DFA



- SCA

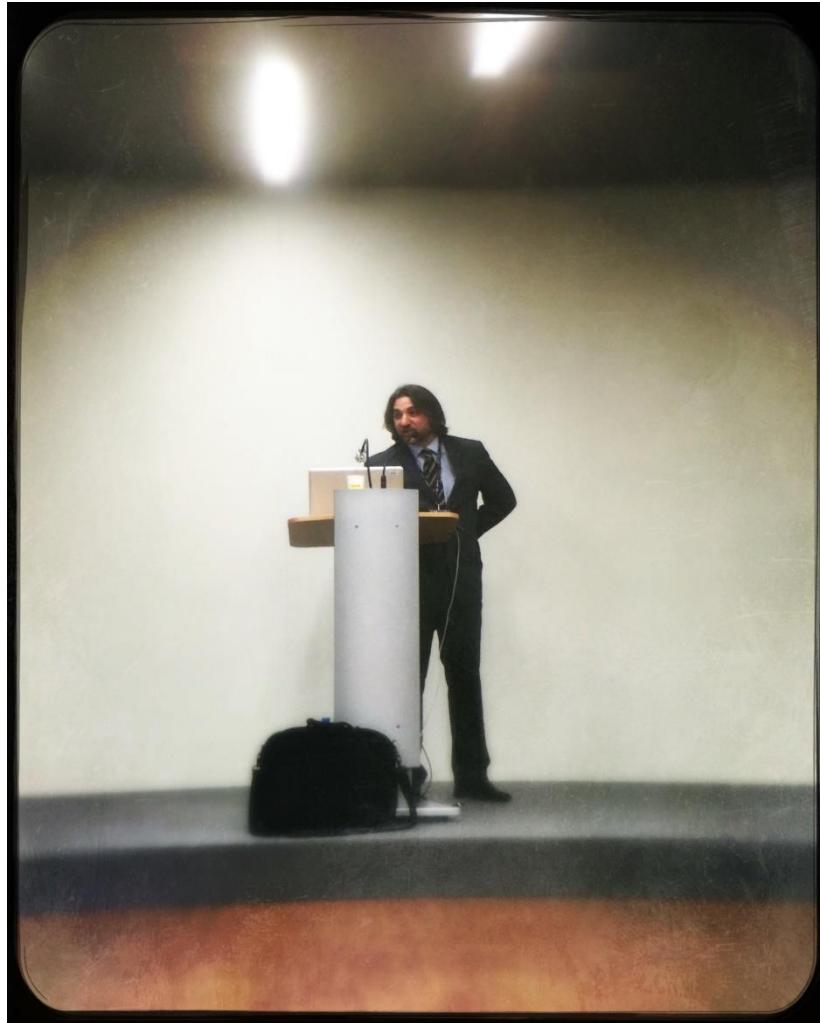


Conférence - Unboxing the White-Box

- Faiblesses de la cryptographie White-box :
 - Attaque SCA très efficace sur WBC standard
 - Requièrè des connaissances en rétro-ingénierie
- Recommandations :
 - Améliorer les protections contre la rétro-ingénierie
 - Renforcer les protections contre l'extraction de clés
- Comment ?
 - Prévenir les dépendances statiques entre clés et intermédiaires
 - Vérification double des données encodées



Conférence - IAEA – The role of the IT security specialists at the International Atomic Energy Agency



Massimiliano Falcinelli

IT Security Systems Unit Head –
International Atomic Energy Agency
(IAEA)

Conférence - IAEA – The role of the IT security specialists at the International Atomic Energy Agency

- L'IAEA est rattaché aux Nations Unies
 - Des collaborateurs de toutes les nationalités
 - Des sites visités tous les jours dans toutes les langues ; presque impossible de mettre en place un filtrage efficace
 - Des échanges entre des zones maîtrisées (réseaux internes) et le reste du monde (ex. ambassade)
 - Comment sécuriser tout ça?
- Le profil des attaquants est assez classique
 - Hacktiviste
 - Script-kiddies
 - Attaques étatiques
- Les attaques aussi 😊
 - Social engineering par mail
 - Intrusion physique pour laisser des messages de revendication ou voler des informations
 - Compromission des sites externes pour récupérer des informations

11:45:00

Conférence - Building Trust by Design



Hoang Bao
@hbao

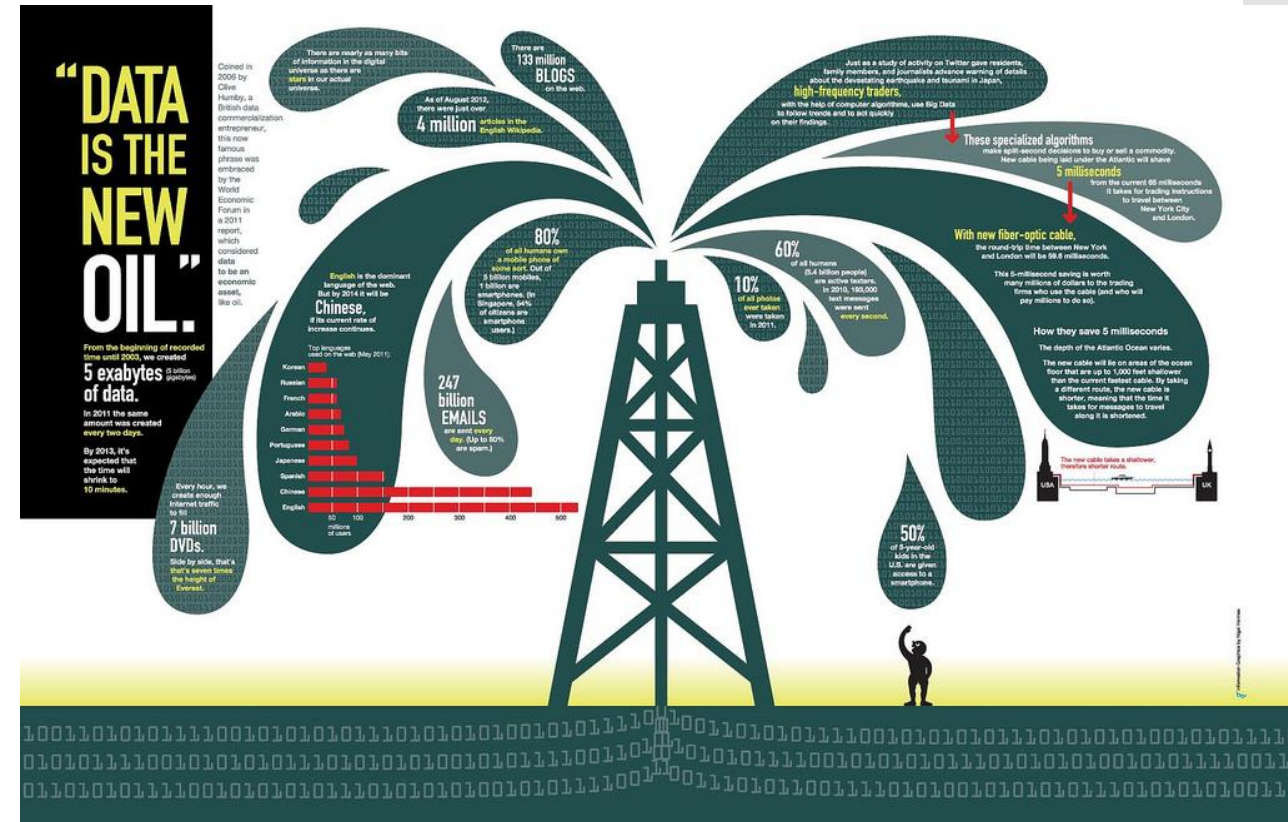
Generation 1.5 working in the world of policy, data, and privacy.

📍 Silicon Valley

📅 Inscrit en avril 2009

Conférence - Building Trust by Design

- Confiance = vie privée + sûreté + sécurité
- Top Domaines à considérer :
 1. Comprendre l'utilisateur final
 2. Collecte de données appropriée
 3. Prévenir et laisser le choix
 - Utiliser outils existants (contrôle IOS, Android)
 4. Améliorer la sécurité
 5. Etendre la valeur des données
- Différences géographique :
 - Droit à l'oubli
 - Accès aux données à caractère personnel
 - Notification de compromission (72 heures)
 - Age majorité



→ Pas d'obligation juridique aux US

Conférence - Building Trust by Design

- Comment améliorer la sécurité :
 - Stockage
 - Rétention et suppression des données
 - Contrôle d'accès
 - Transport (SSL)
 - Journalisation
 - Choix des tiers

- Comment étendre la valeur des données :
 - Anonymisation des données
 - Obfuscation

Conférence - Building Trust by Design

- Conclusion :
 - Priorité donnée à l'utilisateur
 - Contrôles significatifs
 - Intégration de la vie privée, sûreté et sécurité
 - Sécurité = prérequis pour la protection de la vie privée et la sureté

- Age de l'information → Age de l'intelligence



Conférence - 8 security lessons from 8bit games











Florian Hammers

Sales Engineer at Tenable Network Security
Région de Munich , Allemagne | Logiciels informatiques

Actuel Tenable Network Security
Précédent Kaspersky Lab, Computacenter AG & Co. oHG, Class AG
Formation University of Applied Sciences - Ingolstadt

Conférence - 8 security lessons from 8bit games

- La priorité ne doit pas être de vouloir se protéger contre les o-day, mais contre les vulnérabilités déjà connues
- Il propose 8 axes en prenant comme exemple des anciens jeux vidéo
- Pong : La balle ne doit pas passer
 - Réduire la surface d'attaque au maximum
- Tetris : Pour gagner, il faut réfléchir à sa construction
 - Construire son SI sur de bonnes bases
- Asteroids : L'ennemi arrive de tous les côtés
 - Avoir une vue à 100% de ce qu'il se passe sur le SI
- Sonic : Il faut réagir rapidement aux obstacles
 - Être réactif et agile face au changement

Know your Attack Path 	Protect Remote Endpoints 	Reduce Attack Surface 	Focus on Foundational 
Continuous Awareness 	Use Threat Feeds 	Embrace Agility 	Solve Business Problems 

Conférence - 8 security lessons from 8bit games

- Pacman : Fixer des objectifs, les fantômes ne sont pas la priorité
 - Différencier ses besoins de ses envies
- Space Invader : Connaitre les moyens d'attaques des ennemis
 - Faire de la veille et de l'analyse
- Mario : Peach est vulnérable et peut être facilement trompée
 - Bien protéger ses utilisateurs
- Super Mario : Les Goombas sont lents, mais tout le monde se fait avoir
 - Les malwares sont connus, mais sont toujours efficaces, mettre à jour les bases de signature
- Présentation un peu commerciale ;)



12:30:00

REPAS



14:00:00

Conférence - Reversing Internet of Things from mobile applications



Axelle Ap.

@cryptax

Mainly about security, OS, mobile phones. The postings on this page are solely my own opinion and do not represent my employer.

📍 Sophia Antipolis

🔗 wikisec.free.fr

📅 Inscrit en juin 2010

Conférence - Reversing Internet of Things from mobile applications

- Pourquoi analyser les objets connectés ?
 - ≠ matériels
 - ≠ systèmes d'exploitation (Windows, Linux Contiki, RIOT, Tiny OS, Brillo...)
 - ≠ formats de fichier (ELF, BFLT...)
 - Fun ?



• Recon jet



• Beam toothbrush



• Meian Home safety alarm

Conférence - Reversing Internet of Things from mobile applications

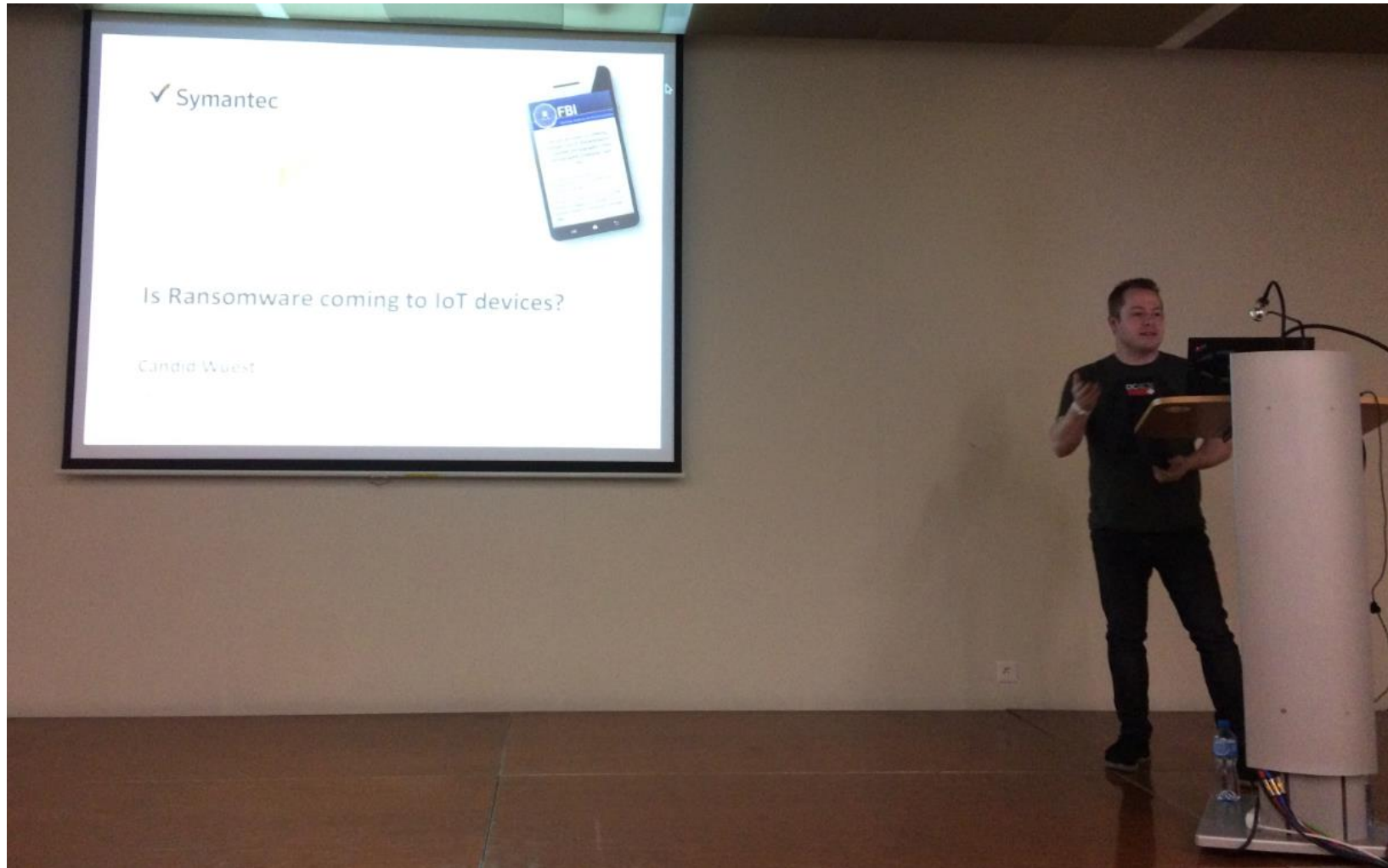
- Pourquoi commencer par la rétro-ingénierie des applications mobiles :
 - Prise en main plus rapide
 - Connaissance plus complète de l'objet audité

- Vulnérabilités trouvées :
 - Recon jet
 - Mot de passe d'archive contenant des événements à synchroniser codé en dur
 - Correctif de l'éditeur → Suppression du mot de passe de chiffrement

 - Meian Home safety alarm
 - Récupération des SMS envoyés dans la boîte d'envoi

15:00:00

Conférence - Ransomware for IoT



candid wueest

@mylaocoon

I work @ Symantec Security Response.
My tweets are my own, and not that of
my employer.

📍 Switzerland area41

📅 Inscrit en octobre 2008

Conférence - Ransomware for IoT

- Motivation lucrative :
 - Ad-clickjacking
 - Ransomware / Locker
 - Infection d'autres appareils
- Scénarios d'attaque :
 - Bloquer l'appareil
 - Chiffrer l'appareil
 - Ingénierie social
- Recommandation :
 - Sécuriser les objets connectés by design
 - Analyser le trafic réseau
 - Ne pas connecter à internet
 - Utiliser de l'authentification forte
 - Ajouter support pour debug

16:15:00

Conférence - From Bored Hacker to Board CISO, a short-n-fun tale



Bruno Kerouanton
@kerouanton

BuildingTrust.in.aConnectedWorld.9c.re
CISO.9c.re ♦
InfosecGlobalSpeaker.9c.re ♦
HonoraryConsul.9c.re ♦
C64demomaker.9c.re ♦
CuriousAboutAll.9c.re ♦

📍 Switzerland, France, USA
🔗 [click.links.above.for.more.info.9c.re](#)
📅 Inscrit en janvier 2010

Conférence - From Bored Hacker to Board CISO, a short-n-fun tale

- Technique d'ingénierie social :



- Analyse de code compilé :



Conférence - From Bored Hacker to Board CISO, a short-n-fun tale

- Comment accepter les risques :



- <https://www.youtube.com/watch?v=gIG3zqvUqJY>

Conférence - From Bored Hacker to Board CISO, a short-n-fun tale

- Goodies :

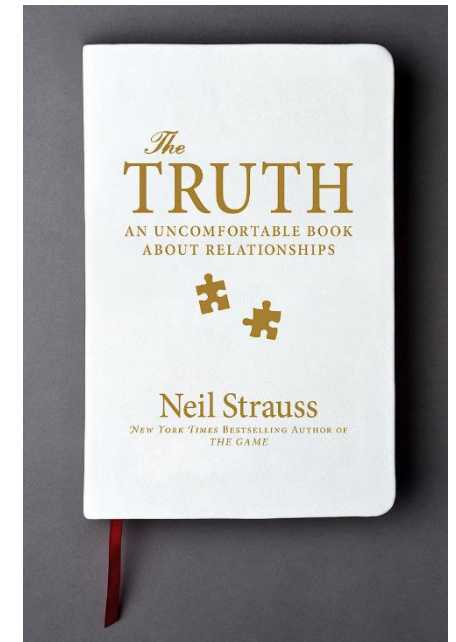
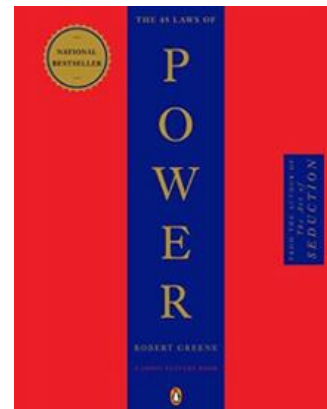


Bruno Kerouanton @kerouanton · 18 mars

A souvenir from my fun final talk at #INS16 @1ns0mn1h4ck. Hope everyone liked it. It was really fun to make!



- Livres :



17:30:00

Apéro sponsorisé



Propriété exclusive d'Intrinsec Sécurité - Reproduction interdite sans autorisation

18:00:00

CTF

- Plus de 200 participants
- 10 h de challenge (jusqu'à 4h)
- Equipes VIP
 - Dragon Sector
 - Tasteless
 - KITCTF
 - Int3pids
 - Shellphish
 - DCUA
- Equipe limitée à 8 personnes



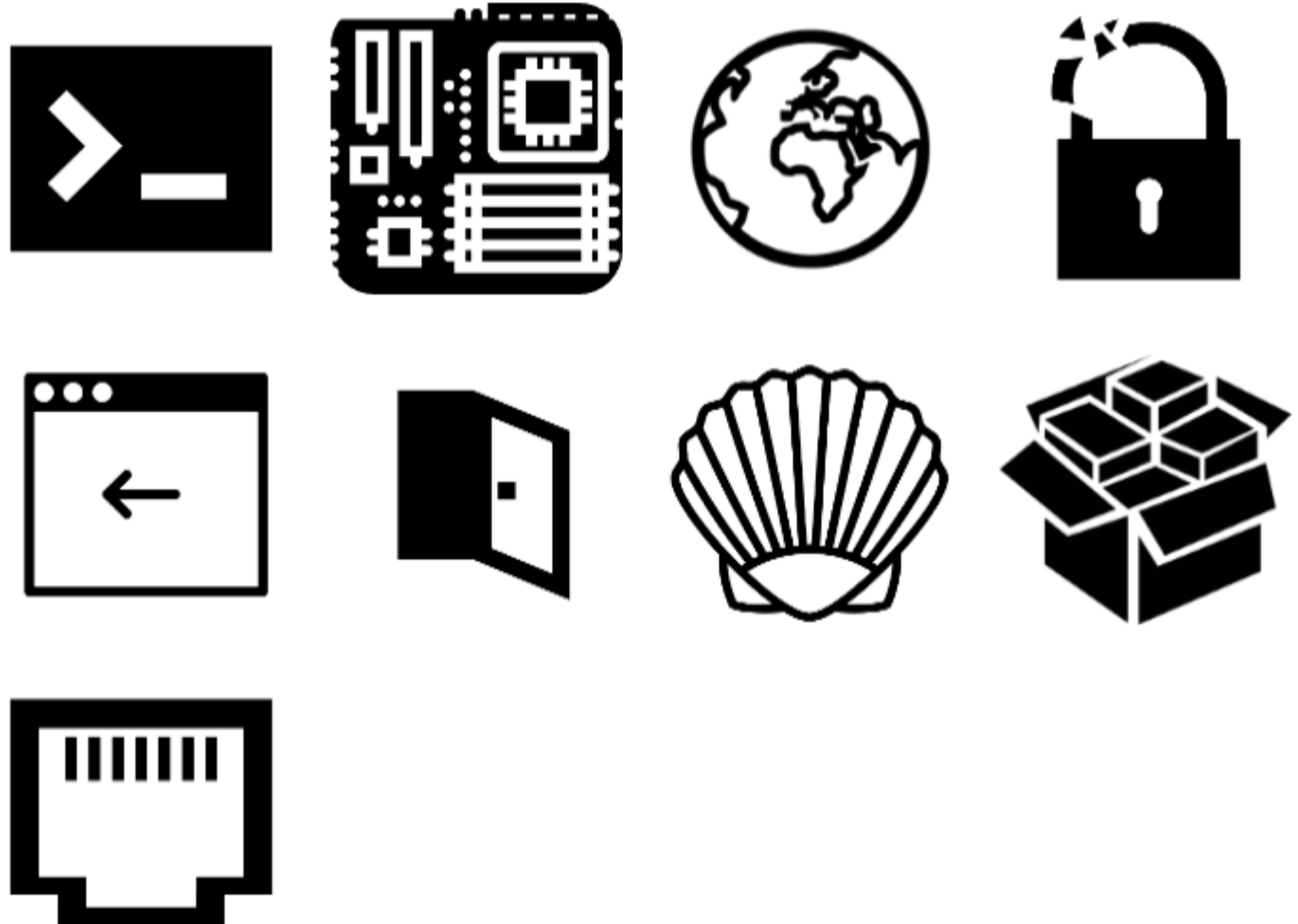
CTF

- 4 Kg d'argent à gagner :
 - (8 * 250g, 8 * 155g and 8 * 100g)



Propriété exclusive d'Intrinsec Sécurité - Reproduction interdite sans autorisation

- Catégories :
 - Backdoor
 - Crypto
 - Hardware
 - Misc
 - Network
 - Pwn
 - Reverse
 - Shellcode
 - Web



CTF

- And the winner is Dragon Sector !!! (Again?)



- Le classement final :

Pos	Team	Score	Last Solved
1	Dragon Sector	169400	Smartdoor2 03:48:12
2	dcua	104350	DrUnk4lyZer I 03:58:36
3	int3pids	94000	Retoasted 02:30:30
4	KITCTF	88200	bIoTch slap 03:19:21
5	p4	75850	OverView of Ideas I 03:35:16
6	H4x0rPsch0rr	69700	robots 02:40:57
7	Shellphish	67950	Smartdoor3 01:28:42
8	Fourchette Bombe	57450	Smartdoor1 03:19:56
9	duks	54000	Smartdoor3 03:31:15
10	Tasteless	53500	Smartdoor3 01:58:57
11	hlcracksngeeks	46850	iBeer 03:58:01
12	mushd00m	42900	smartcat3 03:39:20
13	RGB	37900	CC232 03:10:00
14	khack40	34250	Rostinator 03:08:41
15	Securimag	34250	Smartdoor2 03:45:57
16	0x8F	33850	SafeCRT2 03:40:17
17	ISITDTU	33050	smartcat3 02:42:25
18	Hexpresso	29800	PCAPBleeding 03:09:07
19	cr4zy g0at 0verfl0w	23700	robots 03:43:04
20	FIXME	22100	smartcat3 01:54:26

- Write-ups :

The screenshot shows the GitHub repository page for 'ctfs/write-ups-2016'. The repository is on the 'master' branch and contains a directory structure for various CTF challenges. The commit history shows that the repository was updated 2 days ago by user 'zbetcheckin'.

File/Directory	Commit Message	Time
..		
backdoor	Added Insomni'hack CTF 2016	3 days ago
crypto/pcapbleeding	Added links to local challenge files	3 days ago
hardware	Added links to local challenge files	3 days ago
misc	Added Insomni'hack CTF 2016	3 days ago
network/smartips	Update README.md	2 days ago
pwn	Added links to local challenge files	3 days ago
reverse	Added links to local challenge files	3 days ago
shellcode/superpollute	Added links to local challenge files	3 days ago
web	Added links to local challenge files	3 days ago
.gitignore	Added Insomni'hack CTF 2016	3 days ago
README.md	Added links to local challenge files	3 days ago
scoreboard.jpg	Added Insomni'hack CTF 2016	3 days ago

Merci de votre attention

Questions ?



Site Intrinsec
www.intrinsec.com



Blog Intrinsec sécurité
Securite.intrinsec.com



Twitter Intrinsec
[@Intrinsec](https://twitter.com/Intrinsec)