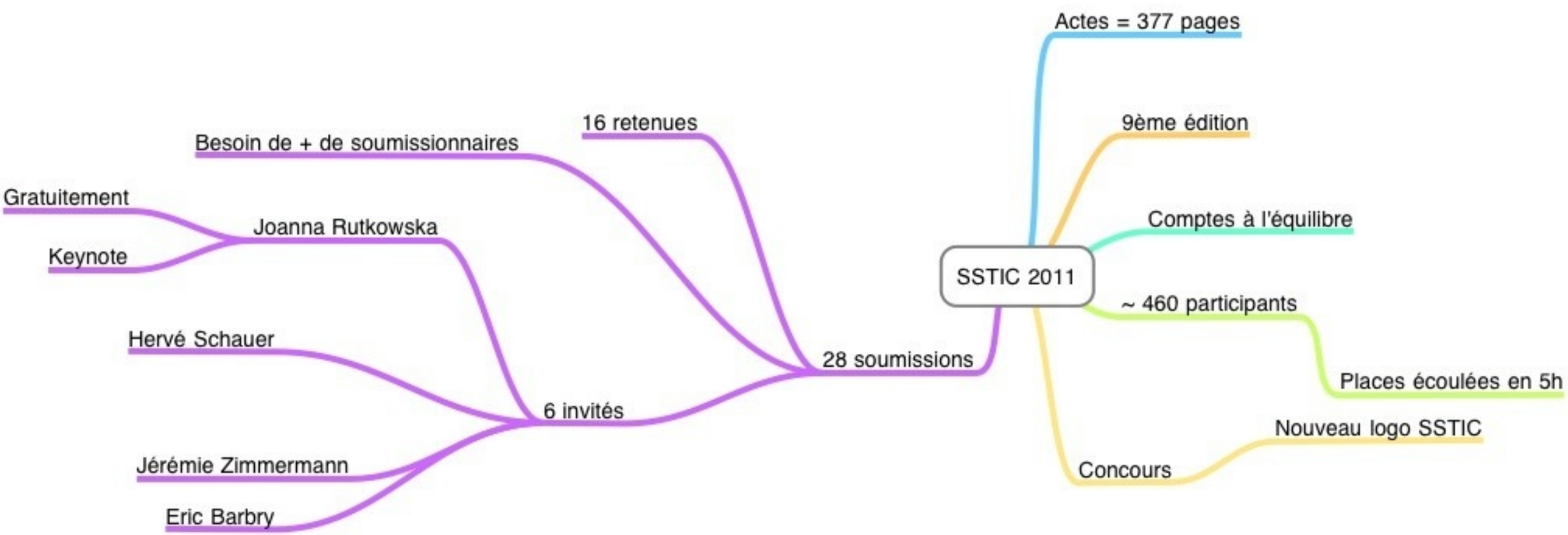
Compte-rendu

OSSIR Paris - 14 juin 2011

Saâd Kadhi <saad.kadhi@hapsis.fr>

1


SSTIC 2011
Actes = 377 pages
9ème édition
Comptes à l'équilibre
~ 460 participants
Places écoulées en 5h
Nouveau logo SSTIC
Concours
28 soumissions
16 retenues
Besoin de + de soumissionnaires
Joanna Rutkowska
Gratuitement
Keynote
6 invités
Hervé Schauer
Jérémie Zimmermann
Eric Barbry

2

Mercredi 8 juin (jour 1)

3

Keynote

Thoughts on Client Systems Security

Joanna Rutkowska, The Invisible Things Lab

"thought-provoking"

4

- Les systèmes client sont nos yeux et nos empreintes
- Notre écran a accès à tout (fait fi de tout chiffrement)
- Notre OS peut nous impersonnifier
- Comment construire la sécurité de ces env. ?

5

- Langages de programmation dits sûrs
- Ex. Microsoft Singularity
- Problèmes liés à la performance

6

- Sécurité réactive
- Correctifs, anti-virus, ...
- Une course continuelle et fatigante

7

- Sécurité par compartimentalisation/isolation
- Une bonne piste à explorer
- Trusted Computing Base minimaliste
- Micro-noyaux, hyperviseurs, sous-sys. non sûrs
- Ex. Xen, Google Chrome, Qubes OS

8

- Isolation par "domaines"
- Réseau / Espace d'addr. / sys. de fichiers,...
- Problème de la GUI
- La plupart n'offre pas d'isolation
- Celle de Windows essaie sans vraiment y parvenir

9

- Sous X11, App 1 peut capturer les saisies clavier effectuées dans App 2

- SELinux et les autres sys. de bac à sable ne peuvent aider

- Pourquoi X.Org ne saisit pas le problème depuis tant d'années ?

10

- L'isolation est un bon principe
- Des exceptions doivent être gérées
- Presse-papiers, partage de fichiers, ...

- Ecole de pensée traditionnelle
- Transferts uniquement depuis une App moins sûre vers une App plus sûre

11

- Traitement d'entrées non sûres
- Qubes inverse le sens des transferts
- App plus sûre vers App moins sûre
- S'appuie sur mém. partagée et un outil similaire à cpio
- Des exceptions doivent être gérées

12

- Ex. copie de lien Web depuis navigateur vers document confidentiel
- Solution ?
- Utilisation de convertisseurs écrits dans un langage sûr
- Comment gérer dans ce cas le presse-papiers ? Ou s'assurer que le résultat de la conversion ne génère pas d'exploitation ?

13

- Quelques limitations
- Cela n'augmente pas le niveau de sécurité des applications
- Décomposer chaque app?
- Projet Capsicum

14

- L'isolation de l'espace d'addr.
- MMU
- Virtualisation
- VT-x / AMD-v / EPT / NPT
- Virtualisation ⩾ MMU
- IOMMU très importante

15

- Qubes OS implémente la plupart de ces idées

- Ce n'est pas un micro-noyau

- Mais tout le reste

- Challenge : comment partitionner notre vie numérique en domaines de confiance ?

16

Slides trop chargées

BitLocker

Parle beaucoup trop vite

Aurélien Bordes, ANSSI

17

- Apparu avec Vista
- Chiffrement intégral DD
- AES-CBC data, AES-CCM metadata
- Windows 7 : utilisation carte à puce possible (pas pour démarrer un vol. sys.)
- Interfaçage avec AD. GPO pour configuration

18

- Conçu pour ordinateur éteint
- Si allumé/verrouillé : menaces réseau (ex. requête WMI) ou physique (lect. mém. sys.), FireWire, *Cold Boot*...
- Utilisateur non admin : pas d'infos pertinentes récupérables

19

- Attaque type Evil Maid (surmédiatisée)
- Modification séquence boot
- Sans TPM : aucune protection n'est efficace
- Avec TPM : les modifications sont détectées

20

- Système stable, bien intégré
- Adapté à un contexte professionnel
- Efficace contre la perte d'une machine
- TPM !

21

Silverlight

Intéressant

Ou comment surfer à travers .NET

Thomas Caplin, SOGETI

Un peu décousu...

22

- .NET framework apparu en 2000, propose C#
- Grande surface d'attaque
- Relativement peu de vulnérabilités depuis sa création

23

- Analyse vulnérabilité d'août 2010 via BinDiff
- 2 instructions modifiées mais gros impact
- Contournement trivial de DEP et ASLR

24

- Silverlight, une piste en or ?
- Peu répandu p/r à Flash
- Permet attaque via Web
- Démo exécution code : FireFox, Internet Explorer (bac à sable), Chrome (prévient si plugin obsolète)

25

- .NET est un énorme composant
- Les exploits contournent DEP et ASLR
- Exploits très stables (absence de heap spraying)
- Pas de bac à sable de Silverlight sous FireFox et Chrome

26

XSSF

Au-delà de la pop-up JS ;-)

Démontrer le danger des XSS
Ludovic Courgnaud, CONIX

27

- Framework d'exploitation XSS
- Développé depuis 1 an
- Utilisable depuis Metasploit, BDD nécessaire
- Objectif : bien expliquer XSS aux commanditaires de pentests

28

- Pourquoi un nouveau framework ?
- XSSed = difficile à installer, nécessite Windows et IIS
- BeEF = complexe à utiliser, code maintenu ?
- HTML 5 augmente la portée des XSS (nouvelles balises HTML, JS Events, Cross-Origin Resource Sharing)

29

- Démonstration : écriture de fichier sur mobile Android

- Fonctionnalité tunnel permettant de faire du XSS sur serveur Intranet

- Contre-mesures XSS ?

30

- Extensions anti-XSS (NoScript...) : restrictifs, quid XSS sur sites de confiance ?

- WAF : nécessite màj règles, difficulté de détecter toutes les variantes

- Filtres XSS des navigateurs : blocage 75% des XSS, pas de support pour les XSS persistants, contournement possible

- Autres : JS sandboxing, auto-échappement (FaceBook XHP, Google CSAS, OWASP JXT)

31

- XSSF non encore officiellement intégré à Metasploit
- Version 2 fin juin 2011

32

Et vos mots de passe sont miens

Rainbow Tables probabilistes

Alain Schneider, LEXSI

Didactique

33

- RT probabiliste i.e. tire partie de la complexité du mot de passe

- Complexité définie selon l'approche de Markov

- Probabilité de transition d'une lettre à une autre

- Mesure d'écart basée sur le produit de toutes les transitions dans un mot

34

- Excellents résultats
- Tests sur base de mots de passe clients et base Rock You
- RT probabiliste de 3.9 GB trouve 87% des mdp Rock You
- Avec base de 2.15 TB, 92%
- Contre-mesure : salez !

35

Pour rétro-concepteurs

Memory Eye

Yoann Guillot, SOGETI

Démo sur un jeu has-been!?!

36

- Outil permettant l'analyse globale d'un programme
- Analyse zone mémoire dynamique
- Application à l'analyse sur un jeu Dwarf Fortress
- Euh... Finalité ?

37

Attaque d'implémentations cryptographiques par canaux cachés

Philippe Nguyen, Secure-IC

38

- Observation d'un composant micro-électronique de crypto

- Trois étapes

    1. Demander à la puce de réaliser des opérations de chiffrement

2. Traiter les rayonnements émis

3. Extraire la clé

39

- Utilisation d'un oscilloscope, d'une antenne et d'un ampli
- Observation de la consommation de courant
- Modèle de fuite (fraction de la consommation globale, prédictible)
- L'utilisation d'une antenne fonctionne beaucoup mieux que l'observation directe du courant

40

- Démonstration
- Récupération d'une clé AES 128 bits en 2 minutes env.
- Contre-mesure : WWDL (Wave Dynamic Differential Logic)

41

Android

Troll Power

Nicolas Ruff, EADS Innovative Works

Il est temps de changer d'ordiphone

42

- OS presque OSS (sauf drivers)
- Base Linux 2.6
- Orienté smartphone
- Principalement ARM
- VM Java Dalvik, bytecode incompat. avec Oracle Java

43

- Quelques chiffres
- Création d'Android Inc. en 2003, rachetée par Google en 2005
- Sur le marché depuis 2007
- 428M de mobiles vendus dans le monde Q1 2011, dont 23.6% de smartphones
- Android = 36%

44

- Modèle de sécurité
- Apps signées (cert auto-signé suffit)
  - Permet la révocation à distance
- Les permissions sensibles doivent être acceptées par l'utilisateur
  - Atomique et irrévocable

45

- Chaque app possède un UID/GID unique
- La Java VM n'est pas une frontière de sécurité

46

- Failles sys
  - Linux, WebKit, lecteur Flash embarqué
- Erreurs logiques
  - Contournement logique, backdoor "null"
- Système de permissions
- Apps boggées
- Aucune permission sur la carte SD

47

- Risque majeur : apps malveillantes
- Très simple
- Le plus dur : se diffuser
- Via une app hôte
- En copiant une app populaire

48

- Démo
- Java Décompiler vs. Good Technologies
- Découverte de la construction du numéro de licence

49

- Quelques points positifs
- Remote kill switch
- Màj over-the-air
- Màj auto des apps à permissions équivalentes

50

Rump day!

Jeudi 9 juin (jour 2)

51

Intérêt pratique ?

Attaques DMA peer-to-peer et contremesures

Fernand LONE SANG

Excellente présentation !

52

- Direct Memory Access
  - Permet à un contrôleur d'effectuer directement des transferts vers mém
- Attaques utilisant des canaux d'E/S
  - USB, FireWire, Ethernet, ...
- Peer-to-peer : utilisation d'un contrôleur pour en attaquer d'autres

53

- Expérimentation portant sur FireWire
- Plusieurs familles de chipsets testés
- Lakeport, Eagleport, Tylersburg
- Northbridge et southbridge
- Différents résultats : R, RW depuis southbridge, depuis Northbridge, ..

54

- Démonstration (vidéo)
- Recopie de flux vidéo entre cible et attaquant via FireWire
- Directement depuis la mém de la CG
- Copie 800x600 pixels à 2 img/s
- Suffisant pour texte

55

- Contre-mesures
- IOMMU
- Virtualisation de la mém. principale
- Contrôle d'accès à cette mém.
- Assure l'isolation
- Ou Access Control Services (uniquement Northbridge Intel)

56

Intérêt pratique ?

Sticky Finger & KBC Custom Shop

Alexandre Gazet

Quand un geek oublie son mot de passe BIOS :-p

57

- L'intervenant oublie son mot de passe BIOS
- Et part à sa quête (ouch)
- Économie // de vente de mdp BIOS
- Comment les mdp BIOS maîtres sont-ils dérivés du numéro de série ?
- Étude porte sur le portable de l'intervenant

58

- Extraction d'un 50aine de modules d'une màj BIOS
- Le contrôleur clavier est impliqué
- KBC expose 140 commandes
- Mdp dérivé du ServiceTag
- Exécution de code KBC
- En pratique, ne sert à rien
- L'intervenant a cependant beaucoup appris ;-)

59

Das Über Hypervisor

Ramooflax

Stéphane Duverger, EADS Innovative Works

Application pour le forensics

60

- Objectif
- Analyser un sys. complet en temps réel
- Machine physique
- Min. de dépendances phy.
- Création d'un hyperviseur à VM unique (bare metal)

61

- Standalone, minimaliste
- Basé sur Intel-VT/AMD-V
- Interaction à distance
- Complexité fonctionnelle déportée sur le client distant
- Comm. distante via EHCI USB 2.0 en DebugPort

62

- Pas mal de limitations rencontrées sur les processeurs
- Incompatibilités, bogues
- Support de fonctionnalités impossible à connaître avant achat processeur

63

- Démonstration
- Faire du GDB en live
- Trouver un processus sur la cible
- Support AMD OK sur Win 7 Pro 32 bits et Debian 5.0 32 bits
- Intel à réécrire

64

Attacking and Fixing PKCS#11 Tokens with Tookan

Graham Steel

Standard, vous avez dit standard ?

Saad's Best Speaker Award

65

- Les tokens PKCS#11 représentent un marché de $5M

- Prix entre $30 et $300 (RSA, ahem)

- Les clés crypto sont stockées et accédées par handle

- Les clés sont stockées avec des attrib. qui en contrôlent l'usage

66

- Le standard PKCS#11 pèse 400 pages
- 1.5 pages dédiées à la sécurité
- Notion de clé sensitive/unextractable
- Chacun implémente le standard à sa façon

67

- Tookan
- Toolkit for cryptoki analysis
- Création d'un modèle formel pour chaque token
- Vérification du modèle avec un model checker (SATMC)

68

- Analyse : génération de clés avec différents attributs
- Vérification SATMC : vecteurs d'attaque
- Ex. déchiffrement clé sensible à l'aide d'une clé avec attributs wrap/decrypt
- Tookan permet aussi de corriger la configuration des tokens

69

- Dur de trouver une configuration sécurisée
- Beaucoup de tokens du marché sont vulnérables (10/18)
- RSA SecurID 800 permet de déchiffrer une clé sensible
- Gemalto SafeSite v2 utilisée dans projet top secret US

70

- Notifications aux fournisseurs
- RSA réactif
- Alladin (ex SafeNet) : c'est dans la roadmap
- Les autres demandent qui d'autre est vulnérable

71

Non, pas vraiment

Peut-on éteindre l'Internet ?

Stéphane Bortzmeyer, AFNIC

72

- Aucune interruption du service de résolution AFNIC depuis sa création
- L'Internet est-il menacé d'arrêt ?
- Des annonces catastrophistes très fréquentes
- Et si on voulait ~~le perturber~~ l'arrêter ?
- Cela dépend du budget

73

- Peleteuse (ou mamie géorgienne équipée d'une pelle) vs. fibres optiques
- Vulnérabilité dans le code IOS
- DDOS
- Abus de pouvoir (Egypte)
- Conclusion : perturber oui, arrêter non

74

- Comment rendre l'Internet plus résilient ?
- Redondance physique
- Éviter les SPOF
- Safe Coding
- Coordination des acteurs de l'Internet
- Surveiller les politiques et les abus de pouvoir

75

Bon récap de DNSSEC & co.

Architectures DNS sécurisées

G. Valadon, Yves-Alexis Perez, ANSSI

SSTIC en avait-il besoin ?

76

- État de déploiement de DNSSEC
- Vue d'ensemble de DNSSEC
- Passage assez rapide sur TSIG et DNSCurve
- Système alternatif : résolution LDAP (interne entreprise)

77

Rump Sessions

78

- Présentations courtes +/- liées à la sécurité
- Chaque intervenant a 4 minutes
- Le public peut le faire partir en applaudissant

79

- Rump SSTIC
- Face cachée des billets SSTIC
- XSS Test Driver
- Digital Forensics XML
- IWKBULKS
- Glubby
- Audits techniques et analyses de risque

80

- Référentiel d'exigences applicables aux prestataires d'audit de la SSI (ANSSI)
- AirScan
- Et si j'ai pas de PC de gamer ?
- Visualiser en sécurité
- Pas vu... pris

Wardriving sur Nintendo DS

Analyse des mdp divulgués par LulzSec

81

- Sécurité de l'implémentation de référence Java Card 2.2.2
- Skyrack, charges utiles ROP
- PanBuster
- NMAP Killer
- Orchids
- Incident Response Methodology

82

- Grandalf
- Security Analysis of The unhackable Victorinox Security Device

Saad's Best Rump

- Direction Générale de l'Armement
- Usages offensifs de XSLT

83

Post
Social Event
(burp)

Vendredi 10 juin (jour 3)

84

Complexe à mettre en œuvre

RRABIDS

Romaric Ludinard, SUPELEC

85

- IDS applicatif (projet DALI)
- Ruby on Rails
- Détection comportementale (je sais...)
- Validation de l'IDS avec une app créée pour cela
- Mal codée (SQLi, modification des paramètres, XSS)

86

- Utilisation de Daikon
- Vérification d'une implémentation p/r à sa spécification
- Instrumentation du code source p/r aux variables contrôlables par l'utilisateur

87

Innovant

Usages offensifs de XSLT

Nicolas Grégoire

Dommage la présentation bling-bling avec Prezi

88

- Exploitation de fonctionnalités dangereuses à des fins d'attaque
- Plusieurs moteurs XSLT ciblés
- libxslt, Xalan-J, Xalan-C, MSXML...
- XSLT 1.0, XSLT 2.0
- XSLT 1.1 (draft), EXSLT (effort communautaire)

89

- Objectifs visés
- Fingerprint du moteur
- Exécution de code
- Création de fichier

90

- Exécution de code dans Xalan-J
  - WebKit, Altova, LifeRay
- Création de fichier dans libxslt
  - WebKit, PHP5
- registerPHPFunctions dans PHP5
- XMLSEC impacté

91

Aspects juridiques de la SSI

Faille de sécurité ou défaut de sécurité

Eric Barbry, avocat

Excellent orateur

92

- Rappel sur les articles 34 et 35 de la loi 78-17
- Données personnelles
- Peu de condamnations
- Peu de contrôles
- Pas de référentiel ?

93

- Les contrôles sont cependant en croissance
- +6% enquêtes CNIL
- L'art. 34 est une obligation de moyens (à priori)

- Mais des problèmes demeurent
- Cas de la sous-traitance
- Quid de l'international ?

94

- Les risques juridiques
- Trois points de vue
- Plateforme / Intrus / Victime
- Vraies conséquences

95

- Fermeture de services
- PR
- Class Action
- Frais d'intervention
- Réclamation client
- Perte de client

96

- A venir très bientôt : notifications en cas de défaut de traitement DP !

- CNIL

- Intéressé(s) si plan de réaction jugé insuffisant par la CNIL

97

- 2 maladies : "normitologie" et "certificologie"
- Nombre important de normes
- Guide CNIL, ANSSI, ENISA, secret défense, ISO 2700x, RGS, ...

- Disposer d'une assurance qualité, pas vraiment
- Rassurant pour un magistrat : ~~on ne savait pas monsieur le juge~~

98

Apprenez le droit !

- Préparation au niveau de l'entreprise
- Amont : socle doc. ISO 27001, audit risque jurid. 27001, plan de conformité
- Aval : guide op. de ctrl, pol. réaction, pol. notification
- Collatéral : proc. sél. prestataires, conditions générales de sécurité, pol. audit des prestataires
- En prévision : demande d'avis CNIL, certification, sensibilisation, assurance

99

Sans slides !

Typologie des attaques contre nos libertés online

Jérémie Zimmermann, la Quadrature du Net

Appel aux citoyens

100

- Internet en tant que bien commun
- On en a tous la gestion
- On doit le protéger
- Attention aux mesures d'exception qui invoquent les émotions (terrorisme, cyberguerre, ...)
- Nécessité d'augmenter les coûts pol. des mauvaises décisions concernant nos libertés

101

Autres présentations

... Et comptes-rendus détaillés

102

- Sys. de stockage en ligne de photos avec confidentialité des données personnelles
- Un framework de fuzzing pour cartes à puce: application aux protocoles EMV
- Sécurité ? (clôture par Hervé Schauer)

- http://www.n0secure.org/
- http://blog.crimenumerique.fr/
- http://sid.rstack.org/blog/

103

Hapsis

45 rue de la chaussée d'Antin
75009 Paris
FRANCE
Tél. : +33 (0)1 53 16 30 60 -
Fax : +33 (0)1 53 16 30 62
Email : contact@hapsis.fr
Web : http://www.hapsis.fr/

104