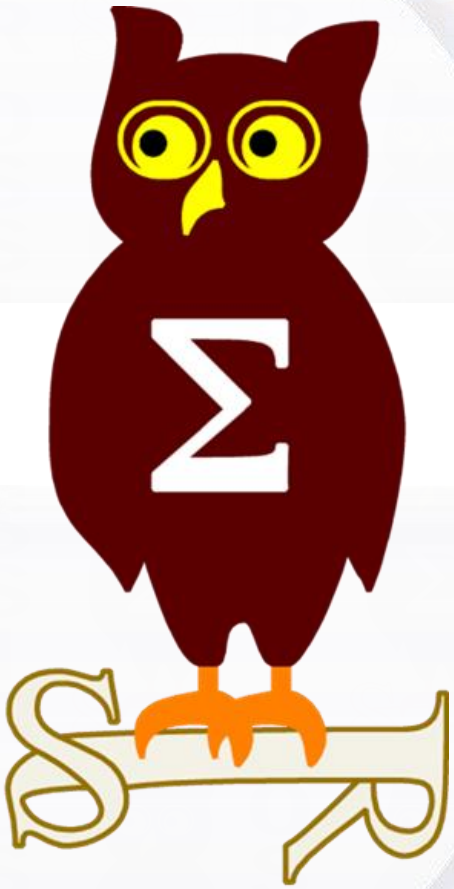


Compte-rendu HIP + NDH

07/07/2015

Préparé par

*Arnaud **S**OULLIE @arnaudsoullie*
*Guillaume **L**OPES @Guillaume_Lopes*

solucom
management & IT consulting

intrinsec

Présentation
Hack In Paris

- Hack in Paris 2015
  - 5ème édition
  - 3 jours de trainings du 15 au 17 juin
  - 10 Trainings
    - A(RM)ndroid/IOS Exploitation par Aditya Gupta et Aseem Jakhar
    - Corealn “Advanced” par Peter Van Eeckhoutte
    - Corlen “Foundations” par Lincoln
    - Hacking Web Applications par Dawid Czagan
    - Hardware HackingLaboratory for Software Pentesters par Yann Allain et Julien Moinard
    - iOS application exploitation par Prateek Gianchandani
    - Mastering Burp Suite Pro par Nicolas Grégoire
    - Offensive HTML, SVG, CSS and other browser-evil par Mario Heiderich
    - Pentesting Industrial Control Systems par Arnaud Soullié
    - Python for Hackers par Gnesa Gianni
  - 2 jours de conférence du 18 au 19 juin
  - 15 conférences et 1 débat

Présentation
Nuit du Hack

- Nuit du Hack 2015
  - 13 ème édition du 20 au 21 juin
  - 12 conférences
  - 15 workshops
  - 1 challenge privé
  - 1 challenge public
  - 1espace de recrutement
    - Yes We Hack
  - 1 NDH kids pour les enfants !

HIP / NDH

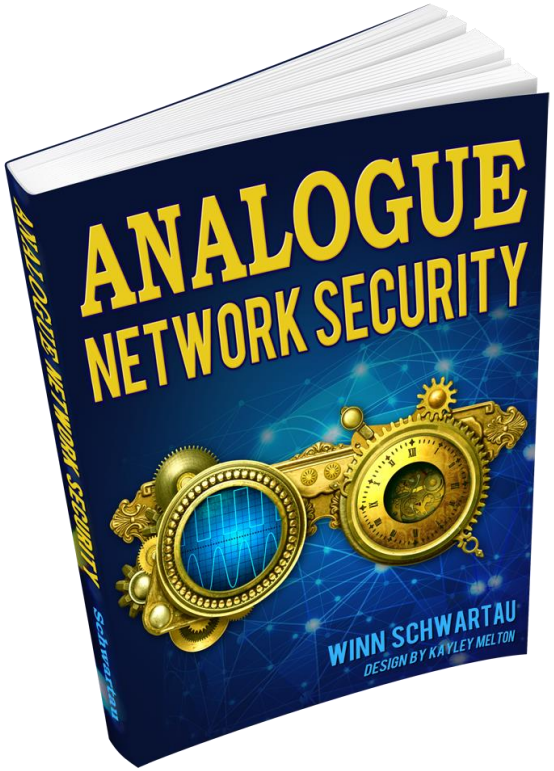
Le lieu

- Académie Fratellini
  - Centre d’art et de formation aux arts du cirque
  - Un chapiteau pour les conférences
  - Une salle pour le challenge et le déjeuner
  - Une salle pour l’espace recrutement (NDH)
  - #infoseccircus

Hack In Paris - Jour 1

Keynote : analogue network security

- Winn Schwartau fait de la pub pour son nouveau livre
- Présente des concepts d'électronique analogique que l'on peut transposer dans la sécurité informatique
- Il a fait part du manque de métrique en sécurité informatique
  - Temps pour se faire compromettre, etc.
- Quelques concepts
  - Boucle de feedback négative : réduction automatique de la bande-passante en cas d'attaque
  - Notion de porte logique "AND" : transposable aux actions d'administration sensibles pour lesquelles on pourrait requérir un quorum d'administrateurs
  - …



⇒ *Théorisation de la sécurité*

⇒ *Difficile d'en tirer des concepts directement applicables*

Hack In Paris - Jour 1

You don’t hear me but your phone’s voice interfaces does

- Même sujet que celui présenté par les auteurs à SSTIC
- L’utilisation d’Interférences Electromagnétiques Intentionnelles permet d’injecter du son au travers des kits mains-libres des ordiphones
- On peut alors, à distance, déclencher des commandes de type “Siri” ou “Ok Google”
- Un téléphone récupéré verrouillé peut ainsi révéler “facilement” des informations sensibles
- Matériel requis
  - USRP
  - Amplificateur
  - Antenne
  - ...pour une portée de 5m (sac à dos) à 20m (camionnette)

⇒ *Sujet intéressant, mais difficile à réaliser en pratique*

Hack In Paris - Jour 1

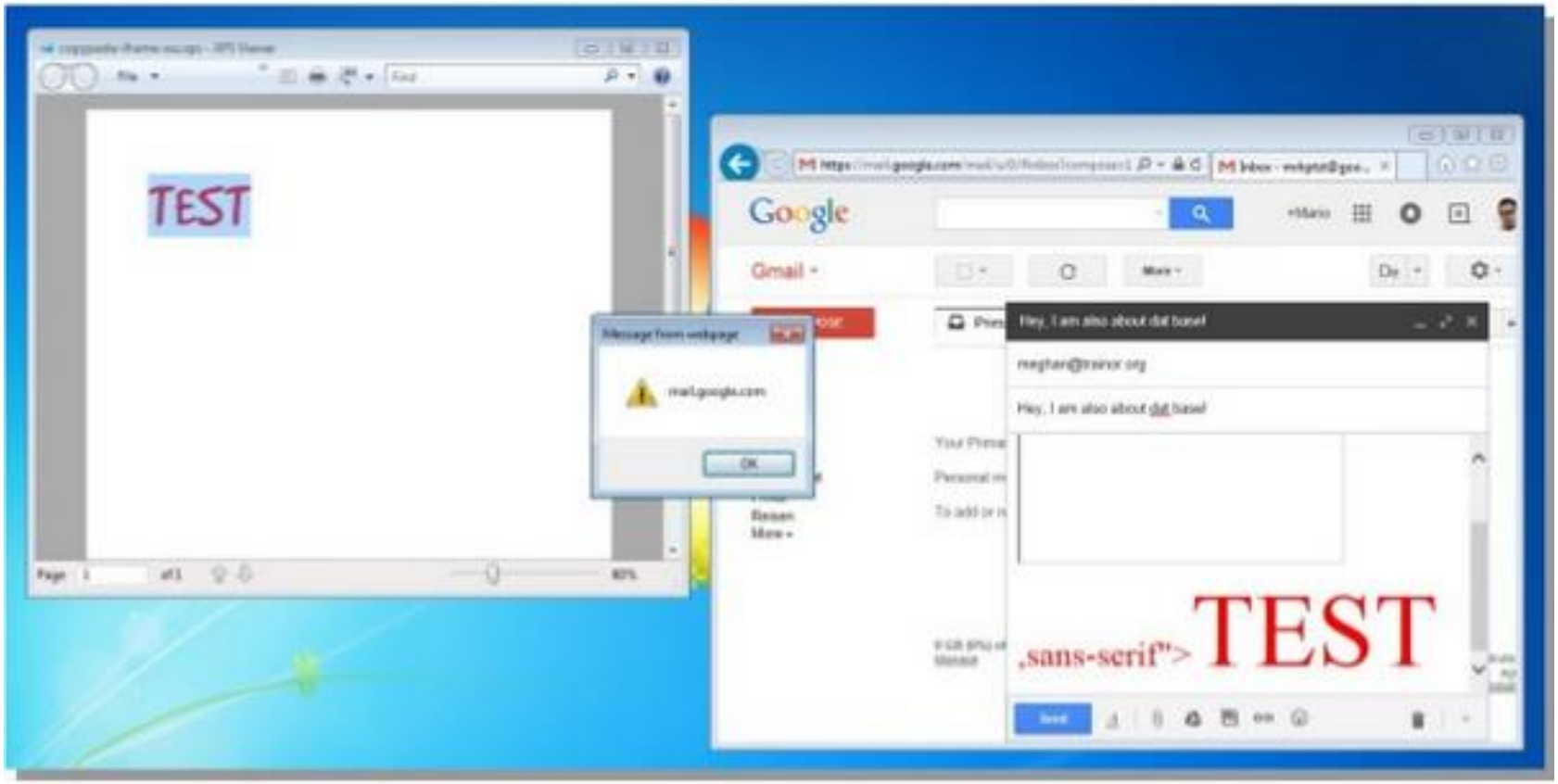
Copy & pest : a case study on the clipboard, blind trust ...

- Présenté par Mario Heiderich (qui a réalisé une thèse sur le XSS)
- Le “clipboard” (ou “presse-papier” en français) peut contenir de nombreux types de données (RTF, HTML, etc.)
- Que se passe-t-il en faisant un “coller” dans un champ texte d’une page web ?
  - Il est possible d’injecter du code JavaScript
- Mais comment insérer du code dans le presse-papier ?
  - Via la fonction “copier”, à partir d’un document malveillant
  - L’exemple d’OpenOffice a été évoqué, il suffit de modifier la police utilisée et de la remplacer par du code HTML
- Il est également possible de faire la même chose en copiant/collant depuis un site web vers une page Word
  - Ce qui est beaucoup plus fréquent
  - En revanche, les possibilités d’exploitation sont réduites

Hack In Paris - Jour 1

Copy & pest : a case study on the clipboard, blind trust ...

- Démonstration réalisée sur Gmail



⇒ *Très bonne présentation avec des cas concrets*

Hack In Paris - Jour 1

Backdooring X11 with much class and no privileges

- Recherche par Matias Katz portant sur la mise au point d'une backdoor discrète sur un poste de travail portable permettant d'y accéder lorsqu'il est verrouillé et sans connaître le mot de passe

- Identification de "dbus" comme élément intéressant
  - Il permet d'intéragir avec les composants physiques

- Deux scénarios démontrés
  - Utilisation d'une clé USB comme dispositif de verrouillage : si la clé est retirée, il n'est pas possible de se connecter au PC, même avec le mot de passe
  - Utilisation de la prise jack comme backdoor : en cas de détection d'une séquence du type "branché/débranché/débranché/branché", déverrouillage du poste sans mot de passe

⇒ *Idée rigolote*

Hack In Paris - Jour 1
Breaking in BAD (I'm the one who doesn't knock)

- Présentation de Jason Street
- Retour d'expérience des techniques d'ingénierie sociale
- Idée : Pourquoi faire des attaques complexes alors qu'on peut obtenir, avec un bon scénario et un peu de politesse, un accès physique aux serveurs qui nous intéressent
- Différents exemples présentés, photos et vidéos de ces exploits
  - Scénario du technicien informatique pour accéder aux équipements d'une banque
  - Scénario du pied dans la porte pour entrer dans un bâtiment de la trésorerie américaine
  - Scénario du faux producteur d'un reportage TV sur une association de charité

⇒ *Retour d'expérience intéressant et en images ☺*

Hack In Paris - Jour 1

Bootkit via SMS : 4G access level security assesment

- Présentation de Timur Yunusov, membre de la SCADAStrangeLove Team
  - http://scadasl.org

- La présentation était assez complète et traitait de différents sujets
  - La sécurité des télécommunications 4G
    - GGSN
    - GPRS
  - La sécurité des périphériques 4G USB et des routeurs
    - Modem USB
    - Routeurs
  - La sécurité des cartes SIM

⇒ Beaucoup d'informations et pas assez de temps pour tout traiter

Hack In Paris - Jour 1

DDOs mitigations' epic fail collection

Florilège de stratégies qui ont échoué pour mitiger une attaque DDoS, par Moshe Zioni

10) Limiter le taux de paquets entrants ⇒ attaques par réflection (téléchargement de fichiers)

9) Supervision incompétente : métriques OK mais site inaccessible

8) Protection des front-ends uniquement

7) Protéger l'intégralité des services : en cas de coupure, tout ser inaccessible

6) Ne pas fournir le certifcat SSL aux provider Anti-DDOS : aucune protection contre les attaques au niveau 7

5) Tout journaliser : épuisement des ressources

4) Filtrage on-demand : peu efficace car pas d'historique du traffic légitime

3) CDN : Limiter aux ressources statiques sinon le CDN fera un DDOS sur les serveurs du client

2) Whitelisting sur l'origine des requêtes : on peut retrouver l'IP et attaquer directement le client

1) Bloquer des sous-réseaux importants : on peut se retrouver à bloquer tout un pays et donc créer soi-même le déni de service

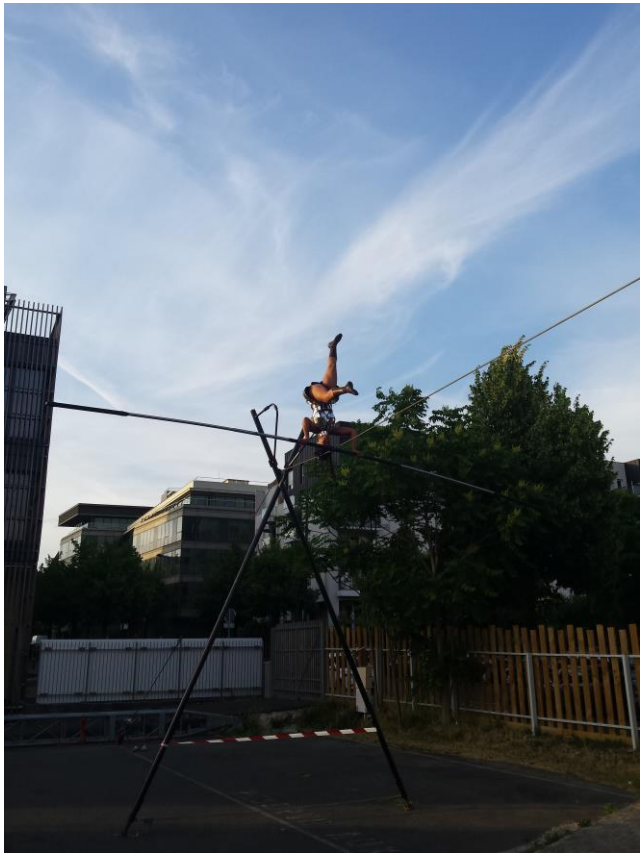
Hack In Paris - Jour 1

Debate : the right to self defense in cyberspace

- Débat de 2 heures sur le fait d'appliquer le concept de légitime défense au niveau informatique

Hack In Paris - Jour 1
Cocktail

- A l'issue de la première journée, un cocktail a été organisé avec quelques animations



Hack In Paris - Jour 2

Keynote : Attacking secure communication: the (SAD) state

- Le constat présenté par l'orateur est simple : "Il est difficile de faire de la cryptographie correctement"
- Évènements marquants en Egypte et à Hong Kong nécessitent de plus en plus d'assurer la confidentialité des communications
- Pas assez de projets qui assure la confidentialité des communications
  - S/MIME : impose d'avoir une autorité de certification
  - PGP : difficile à utiliser et l'échange de clés s'effectue encore à la main en 2015 :)

- ProtonMail
  - NSA proof (basé en Suisse)
  - 2 mots de passe : 1 mot de passe pour l'authentification et 1 mot de passe pour déchiffrer les emails
  - Vulnérabilités identifiées
    - Cross Site Scripting stocké et volatile
    - Cross Site Request Forgery
    - Nombreux services d'administration visibles (Dell Manage, VNC, FTP, SSH, etc.)

Keynote : Attacking secure communication: the (SAD) state

- Tutanota (similaire à ProtonMail)
  - Vulnérabilités identifiées
    - Cross Site Scripting dans l'objet du mail
    - Pas de possibilité de se déconnecter car clé de session statique
    - Cryptographie "maison" : RSA + AES
    - Pas de vérification des clés de chiffrement

- SilentCircle (alternative à Dropbox)
  - Des vulnérabilités ont été également identifiées
  - Mais elles sont en cours de correction…

- L'Electronic Frontier Foundation tient à jour une liste d'outils pour sécuriser les communications
  - https://www.eff.org/secure-messaging-scorecard

⇒ Résultats intéressants et état des lieux assez concret de la cryptographie

Hack In Paris - Jour 2

Server-side browsing considered harmful

- Nicolas Grégoire nous présente les résultats obtenus pour la participation à certains « bug bounties »
- Démonstration d'attaques SSRF : Server-Side Request Forgery : l'attaquant arrive à forcer le serveur à effectuer une requête sur une ressource tierce
- Possibilité de scanner le réseau interne, mais aussi d'accéder à des ressources standard sur les différents fournisseurs de cloud
  - Meta-data server : http://169.254.169.254/
  - /latest/meta-data/iam/security-credentials/ : éléments d'authentification temporaires sur AWS
- Ensuite, de nombreux exemples de contournement de listes noires ont été évoqués

http://425.510.425.510/

http://2852039166/

http://7147006462/

http://0xA9.0xFE.0xA9.0xFE/

http://0xA9FEA9FE/

http://0x41414141A9FEA9FE/

http://0251.0376.0251.0376/

http://0251.00376.000251.0000376/

- And you can mix them
  - http://425.254.0xa9.0376/
  - Decimal (w/ and w/o) overflow + hex + octal
- Or convert only parts of the address
  - http://0251.0xfe.43518/
  - Octal + hex + 2-byte wide dotless decimal

Hack In Paris - Jour 2

Server-side browsing considered harmful

- Bugs identifiés (liste non exhaustive)
  - Stripe (500 $)
    - Contournement d'une blacklist via une redirection
  - Prezi (4 500$)
    - Accès à des ressources internes (2 000$)
    - Accès aux fichiers AWS (2 000$)
    - Contournement de la restriction IP (500$)
  - Parse (20 000$)
    - Accès aux services internes via une redirection

⇒ *Conférence très intéressante avec des astuces ☺*

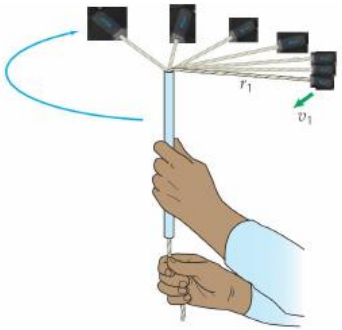
Hack In Paris - Jour 2

Fitness tracker: hack in progress

- Présentation d'Axelle Aprville sur le bracelet Fitbit Flex
  - Bluetooth Low Energy
  - Accéléromètre
  - Enregistre le nombre de pas (marche et course) et la qualité du sommeil

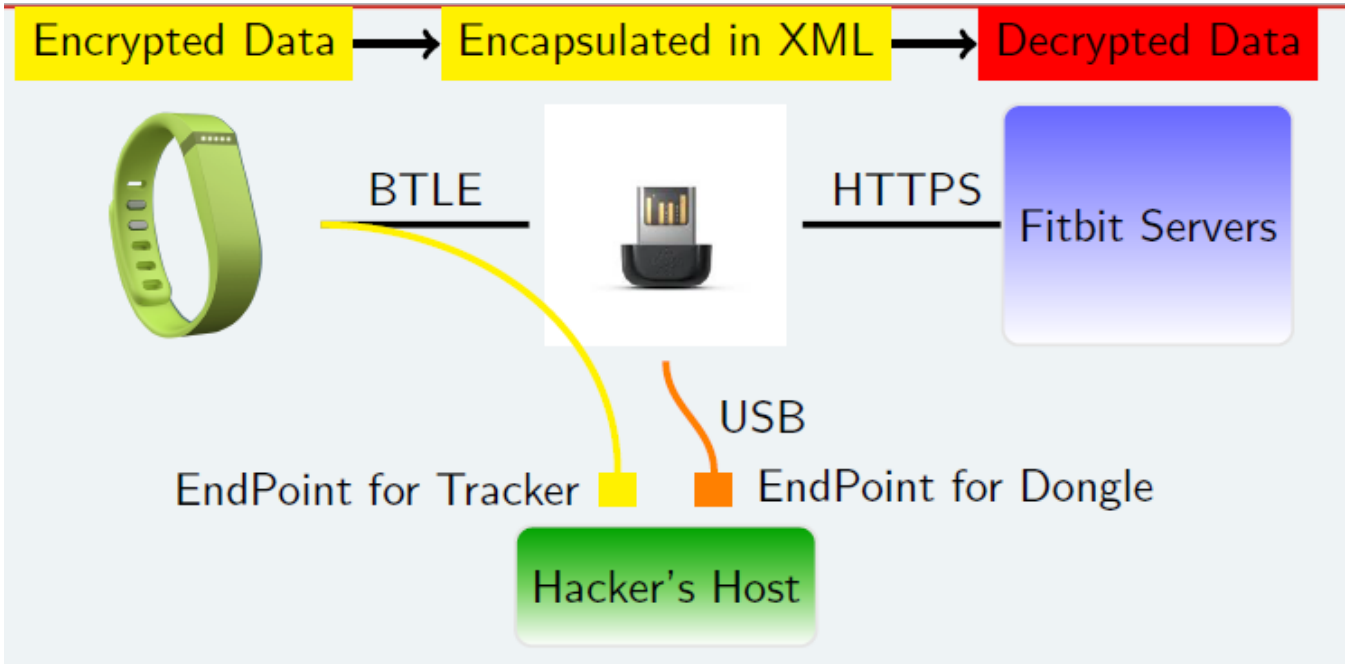
- Problèmes de confidentialité notamment sur l'activité sexuelle des utilisateurs

- Il est possible de tromper la sonde sur le nombre de pas ;)



Fitness tracker: hack in progress

- Architecture de la solution



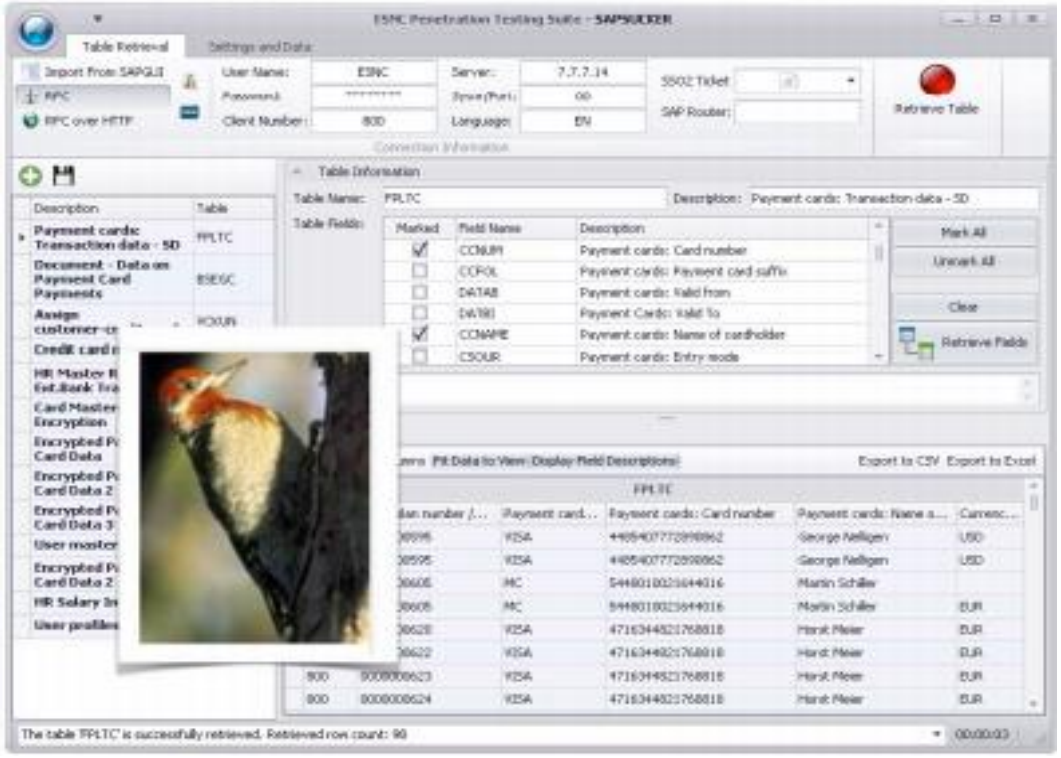
- Reverse engineering du protocole de communication
  - Des failles ont été identifiées mais en discussion avec l'éditeur
  - Le fonctionnement complet n'a pas encore été élucidé
- Utilisation du bracelet pour faire de l'entropie ;)

Hack In Paris - Jour 2

SAP Security: real life attacks to business processes

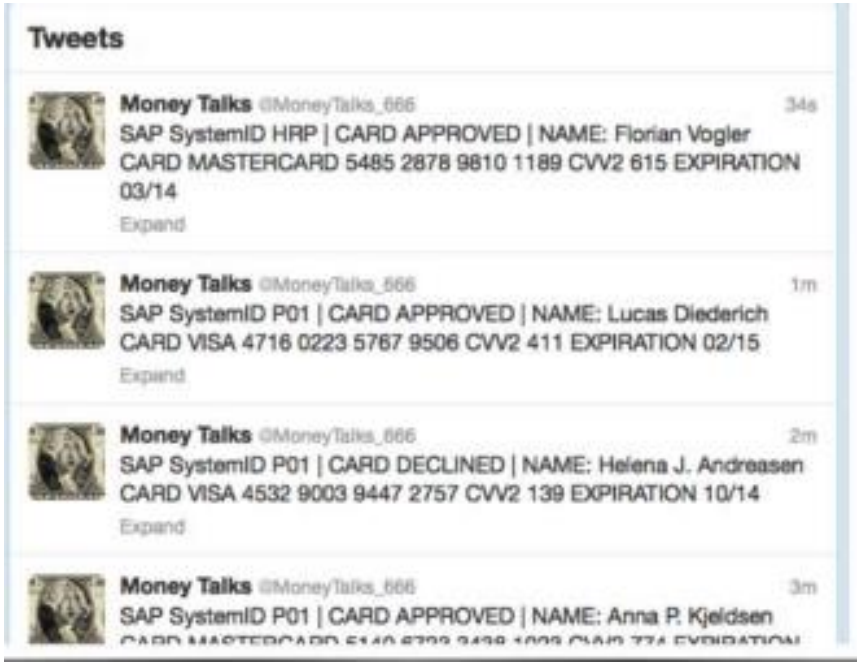
- La sécurité des systèmes SAP est globalement peu prise en compte, et pourtant ces systèmes s'interfacent avec l'intégralité du SI et manipulent des données sensibles

- Démonstration d'exécution de code arbitraire sur un système SAP via l'outil "SAPSucker" (vulnérabilité corrigée)



SAP Security: real life attacks to business processes

- Que peut-on faire sur un systèmes SAP ?
  - Exemple : changer le RIB des fournisseurs pour recevoir le montant des factures automatiquement
- Les systèmes SAP manipulent également fréquemment des données de cartes bleues
  - Plus de 50 tables différentes dans SAP peuvent contenir ce type de données
- En cas de conformité PCI-DSS, ces données sont chiffrées évidemment mais en cas de compromission comme celle démontrée, il est tout à fait possible de faire appel à la fonction de déchiffrement pour récupérer les données en clair



Hack In Paris - Jour 2

Oracle peoplesoft applications are under attack!

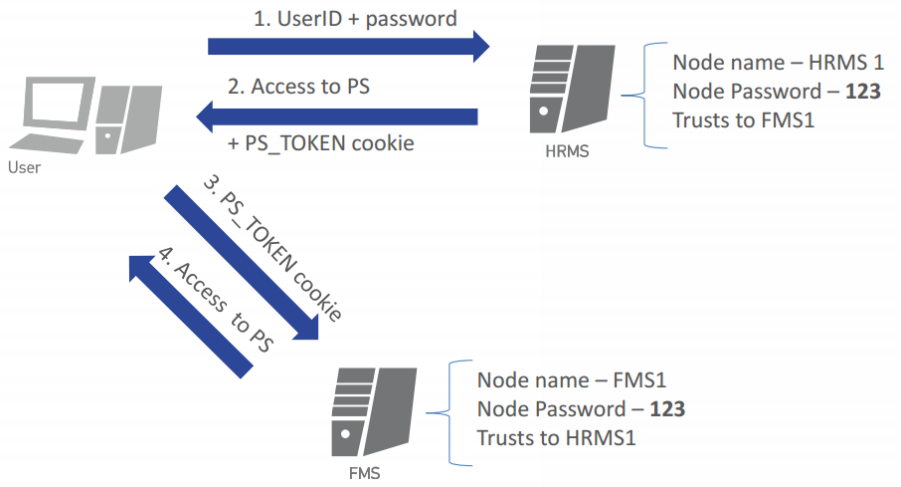
- Oracle PeopleSoft est un logiciel destiné aux entreprises et permettant la gestion des ressources humaines, de la supply chain, de la relation client (CRM)

- La solution repose sur le serveur applicatif WebLogic, mais la version packagée avec PeopleSoft n'est pas sécurisée par défaut

- Démonstration d'une vulnérabilité de contrôle d'accès dans Weblogic, permettant à un utilisateur standard d'ajouter une application et donc d'exécuter du code sur le serveur

Hack In Paris - Jour 2
Oracle peoplesoft applications are under attack!

- Problème majeur sur les cookies de sessions de PeopleSoft
  - Valeur pas aléatoire…
  - …mais un hash de différentes valeurs (timestamp, username, mot de passe de serveur)
  - En “cassant” le SHA-1, on retrouve le mot de passe du serveur et on peut alors générer un cookie pour un autre nom d’utilisateur….
  - Pire, il est possible d’obtenir un cookie “visiteur”, sans authentification, ce qui permet également de casser le SHA-1



Hack In Paris - Jour 2
Exploiting TCP timestamps

- Présentation de Veil Hailperin sur les timestamps TCP

- Les timestamps permettent d'obtenir des informations sur la machine distante
  - Calculer l'uptime et ainsi déterminer son niveau de patch
  - Obtenir la version du système d'exploitation
  - Identifier des services cachés
  - Identifier le nombre d'équipements derrière un NAT

- Pas de solutions proposées et sans doute pas de solution du tout pour éviter cette "fuite" d'informations

- Un script python a été développé pour analyser les résultats d'un scan Nmap et ainsi déterminer le nombre d'adresses IP derrière un NAT
  - https://github.com/luh2/timestamps

⇒ *Présentation old school*

Hack In Paris - Jour 2

Simple Network Management PWND

- Deral Heiland et Matthew Kienow nous ont parlé de SNMP
- La première partie s'est concentrée sur la présentation du protocole
  - Comment effectuer des requêtes SNMP ?
  - La différence entre les versions 1 et 2 ?
  - A quoi sert ce protocole ?
  - Ce qu'est un OID et une MIB ?
- Lors de la seconde partie, les 2 chercheurs nous ont montré qu'il était possible de retrouver des informations sensibles sur des équipements réseau et imprimantes via le protocole SNMP
  - Clés Wifi
  - SSID des réseau Wifi
  - Identifiants et mots de passe des interfaces d'administration
  - Identifiants et empreintes de mots de passe
- Des scripts Perl ont été développés afin de faciliter l'extraction et l'identification de telles informations
  - https://github.com/dheiland-r7/snmp
- En conclusion
  - Désactiver SNMP si non utilisé
  - Utiliser la version 3 de SNMP
  - Les MIB SNMP ne doivent pas contenir d'informations sensibles (mot de passe, clés Wifi, etc.)

Hack In Paris - Jour 2

Revisiting ATM vulnerabilities for our fun and vendor's profit

- Olga Kochetova et Alexey Osipov ont présenté leurs travaux sur la sécurité des distributeurs automatiques de billets, très semblable à la conférence présentée à la BlackHat Europe l'an dernier

- De nombreux distributeurs utilisent encore Windows XP, et certains sont accessibles sur Internet (vérifié en live durant la conférence)!

- Les distributeurs sont composés de deux parties :
  - La zone « service » : contient le PC, les éléments réseau,etc
  - La zone « safe », qui contient les cassettes de billet

- Il est relativement facile de crocheter la serrure de la zone de service

- On peut alors insérer un équipement type Raspberry Pi, connecté en USB

- Un peu de Google Hacking et de reverse pour comprendre les commandes XFS nécessaires à la distribution de billets

- On peut alors piloter le distributeur à distance et récupérer tous les billets

Nuit du hack
Conférences / Workshops / YesWeHack / Kids

- En vrac sur les conférences
  - La keynote de Guillaume Poupard qui a présenté le travail de l'ANSSI et le problème de température dans les locaux ☺
  - PlagueScanner l'outil qui permet de scanner un fichier par plusieurs antivirus
  - L'impression de clé en 3D : le grand classique de la nuit du Hack
  - Des statistiques sur les malware Android
- En vrac les workshops
  - Le lockpicking comme tous les ans ;)
  - Le confessional de Zataz
  - Présentation de Radare2 (alterntive à IDA)
    - http://maijin.fr/slides.pdf
- Les bug bounty : DenyAll et Qwant

Le succès du « Bug Bounty » DenyAll à la Nuit du Hack 2015

Pendant l'évènement « Nuit du Hack 2K15 » qui s'est tenu à Paris le 20 et 21 Juin dernier, le premier « Bug Bounty » organisé par DenyAll a vu 2 000 experts tester ses pare-feux applicatifs Web. Les données collectées seront analysées en détail pour optimiser davantage la pertinence et l'efficacité des moteurs de sécurité applicative de DenyAll.

HIP / NDH
Conclusion

- Lieu moins confortable que DisneyLand mais assez sympa
- Grosse différence d'ambiance entre HIP et NDH
  - HIP : 250 personnes
  - NDH : 1 500 personnes

- Le prix d'entrée de la NDH est abordable, quant à HIP il est facile de se faire inviter

- Compte-rendu d'HIP
  - http://www.securityinsider-solucom.fr/2015/06/hack-in-paris-2015-notre-compte-rendu.html
  - http://securite.intrinsec.com/2015/07/01/hack-in-paris-2015-premiere-journee/
  - http://securite.intrinsec.com/2015/07/01/hack-in-paris-2015-seconde-journee/

- Podcast
  - http://www.nolimitsecu.fr/hip-ndh-2015/

Questions ?