THE CONTROL OF TECHNOLOGY BY NATION STATE: PAST, PRESENT AND FUTURE

The (unofficial) case of Cryptology and Information Security

Eric FILIOL – ESIEA (C + V)O Lab – filiol@esiea.fr

http://sites.google.com/site/ericfiliol/

http://sites.google.com/site/esieanismaster/

INTRODUCTION

- Question:

Just imagine that if inconditionnally secure systems (computer, information security…) would be possible (theoretically AND practically), would it be desirable to use or authorize it?

- The answer is no due to
  - National Security Issues (Intelligence, Defense, Police, Justice…)
  - Strategic dominance, information assurance…
  - Economic warfare & dominance (since 1989)

QUELQUES FAITS ILLUSTRATIFS

- Backdoor chinoises …
- … et US

RuggedCom confirme la présence d'une backdoor dans ses équipements

01/05/2012 à 18:36

Ah bin ça y est! RuggedCom, le spécialiste canadien dans le matériel de communication associé à Siemens, a confirmé que ses produits basés sur le système d'exploitation Rugged (ROS) contiennent une backdoor.

Selon Jim Slinowsky, les versions 3.2.x et antérieures de ROS permettraient l'accès via une backdoor à la console en utilisant les protocoles et services SSH, HTTPS, telnet et shell distant (rsh). Les versions 3.3.x et postérieures désactivent telnet et rsh.

La société affirme qu'elle va sortir de nouvelles versions du firmware ROS qui supprimeront le compte "usine" et désactiveront aussi les services telnet et rsh par défaut. Les mises à jour pour ROS 3.7, 3.8, 3.9 et 3.10 seront mises à disposition "dans le courant de la semaine prochaine". Il est vivement conseillé que les utilisateurs exécutant une version de ROS antérieure à la 3.7 mettent à jour leur firmware vers la version la plus récente.

Cependant, RuggedCom dit qu'il va "mettre en place des mises à jour pour les versions précédentes sur un cas par cas" (pour ceux qui ne peuvent pas mettre à jour). En outre, il prévoit de publier une nouvelle version de son logiciel RuggedExplorer visant à "mettre plus facilement à jour le firmware et modifier les paramètres de configuration ROS qui aideront les utilisateurs pour le déploiement sur de grands réseaux."

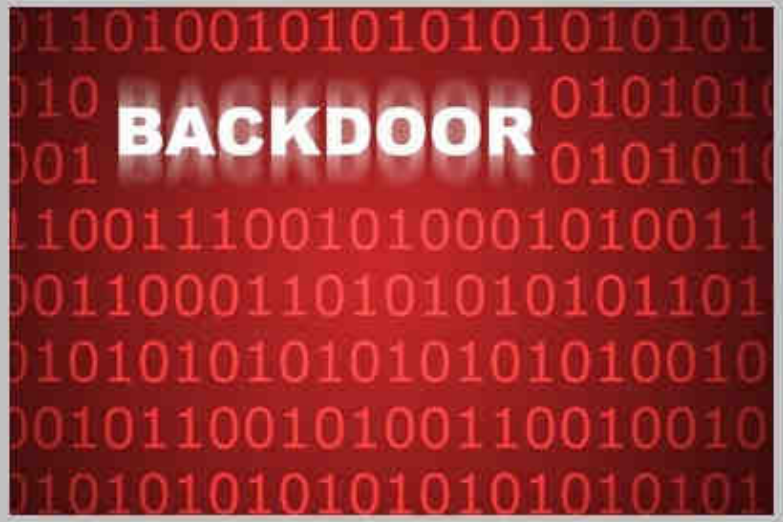
Je viens de voir que de plus amples informations au sujet de cette backdoor, y compris une liste complète des switchs et serveurs touchés, peuvent être trouvés dans le bulletin de sécurité de RuggedCom.

CR@ZY'S WEBSITE

STAY TUNED & POWERED !

Backdoor dans des équipements réseau industriels

26/04/2012 à 16:59



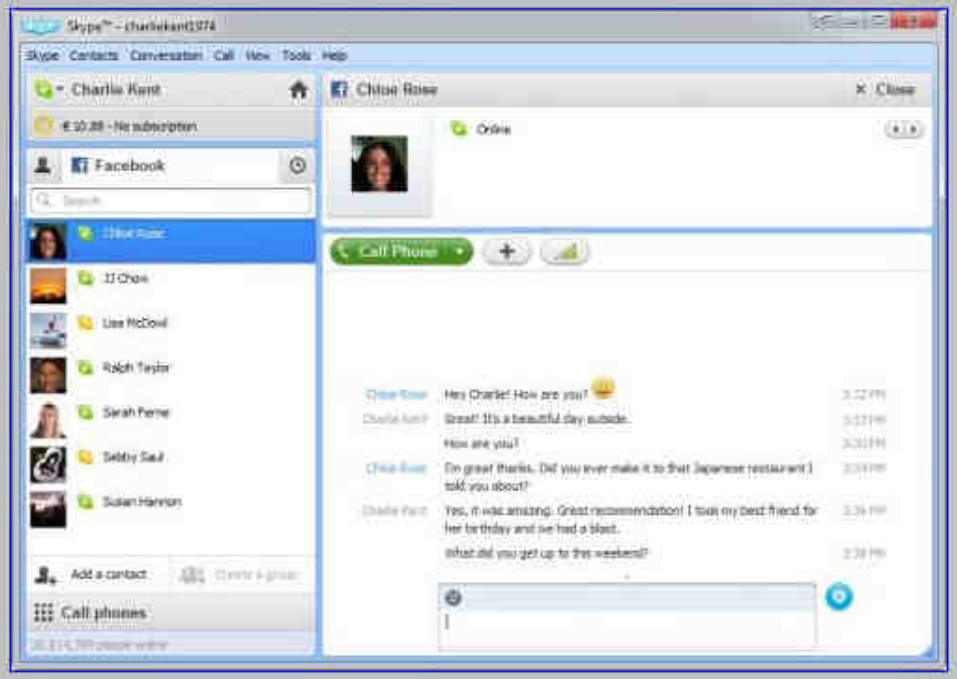
Le **Rugged Operating System (ROS)**, un système d'exploitation créé par les développeurs de RuggedCom, contient une backdoor qui était jusqu'à ce jour méconnue.

RuggedCom, une filiale de Siemens, est spécialisée dans les équipements réseau de grande qualité pour les "environnements difficiles". Ce genre d'équipement, tels que des switchs ou des serveurs, est recommandé dans des centrales électriques, centrales nucléaires, des raffineries de pétrole, les milieux militaires et les systèmes de surveillance du trafic. Ces divers équipements sont très utilisés dans le monde et en particulier dans le domaine militaire.

Microsoft : vers une automatisation de la surveillance du réseau Skype ?

Contrainte réelle, brevet qui fâche

Depuis que Microsoft a racheté Skype pour la modique somme de 8,5 milliards de dollars, la firme n'a pas réellement communiqué sur ses projets futurs. On sait que la technologie VoIP sera intégrée dans un certain nombre de produits, mais l'éditeur n'a toujours pas précisé lesquels, et on s'étonne de n'avoir vu Skype arriver en bêta sur Windows Phone 7 que tout récemment. Mais il est un point qui pourrait faire parler de lui : l'inclusion dans le client d'une porte dérobée pour autoriser les écoutes légales.



Cette capacité ne doit rien au hasard. La majorité des pays dispose d'un concept de « Lawful interception », c'est-à-dire l'interception légale par les autorités des communications. La procédure est déclenchée dans le cas par exemple d'écoutes téléphoniques et est largement utilisée par les forces de police. Mais ce qui était valable pour la téléphonie traditionnelle l'est tout autant pour la voix sur IP.

Il y donc une obligation légale pour Microsoft de permettre ce genre d'écoute. Aux États-Unis, la loi est définie par le CALEA (Communications Assistance for Law Enforcement Act). Cependant, Microsoft semble vouloir aller plus loin en proposant volontairement une technique pour laquelle la firme a par ailleurs déposé un brevet en décembre 2009.

Microsoft estime que les Plain Old Telephone Services utilisés actuellement sont tout simplement archaïques et ne peuvent pas remplir

Microsoft : vers une automatisation de la surveillance du réseau Skype ?

Contrainte réelle, brevet qui fâche

Depuis que Microsoft a racheté Skype pour la modique somme de 8,5 milliards de dollars, la firme n'a pas réellement communiqué sur ses projets futurs. On sait que la technologie VoIP sera intégrée dans un certain nombre de produits, mais l'éditeur n'a toujours pas précisé lesquels, et on s'étonne de n'avoir vu Skype arriver en bêta sur Windows Phone 7 que tout récemment. Mais il est un point qui p

Ecoutes électroniques : le FBI veut instaurer un « backdoor » pour les services Internet

Aux Etats-Unis, le FBI propose une règle visant à rendre les principaux services Internet à vocation interpersonnelle (VoIP, réseaux sociaux, messagerie…) compatibles avec un « extra-code » pour faciliter les enquêtes.

Le 7 mai 2012 par Philippe Guerrier 0 Commentaire
C'est une proposition difficile à accepter de la part des groupes Internet.

Aux Etats-Unis, le **FBI** a demandé à des acteurs comme Google, Microsoft, Facebook ou Yahoo de laisser une porte ouverte à un logiciel de type « backdoor » facilitant les écoutes électroniques.

Dans le cadre d'enquêtes fédérales liées à des activités illégales (organisations criminelles, lutte anti-terrorisme…), les agences en charge de la sécurité semblent rencontrer des difficultés pour établir des systèmes d'écoute sur les outils de téléphonie sur Internet.

Le cas de Skype (passé sous la bannière Microsoft) était déjà considéré comme problématique.

Son usage est désormais généralisé dans le monde entier et les services de renseignement et de police du monde entier semblent rencontrer des difficultés pour suivre ce qu'il se dit via ce logiciel de téléphonie sur Internet.

Mais la direction juridique du FBI souhaite aller plus loin à travers une ébauche d'une proposition de loi censée faciliter sa tâche.

Elle souhaite demander à toutes les sociétés Internet exploitant des réseaux sociaux, des services de voix sur IP, des outils de messagerie instantanée et des webmails d'accepter le principe d'une « compatibilité technique » pour les écoutes électroniques.

Selon CNET.com qui a interrogé un représentant de l'industrie IT qui parle sous le couvert de l'anonymat, il s'agirait d'inclure cet « extra-code » à tous les services de communication interpersonnelle.

C… légale
p… utilisée
par les forces de police. Mais ce qui était valable pour la téléphonie traditionnelle l'est tout autant pour la voix sur IP.

Il y donc une obligation légale pour Microsoft de permettre ce genre d'écoute. Aux États-Unis, la loi est définie par le CALEA (Communications Assistance for Law Enforcement Act). Cependant, Microsoft semble vouloir aller plus loin en proposant volontairement une technique pour laquelle la firme a par ailleurs déposé un brevet en décembre 2009.

Microsoft estime que les Plain Old Telephone Services utilisés actuellement sont tout simplement archaïques et ne peuvent pas remplir

Le Monde.fr
Technologies

Facebook enregistre des informations après la déconnexion de l'utilisateur

LEMONDE.FR | 26.09.11 | 17h07 • Mis à jour le 26.09.11 | 18h09

La page d'accueil du réseau social Facebook.AFP/KAREN BLEIER

Se déconnecter ne suffit pas : d'après les observations de l'Australien Nik Cubrilovic, spécialiste en sécurité informatique, Facebook continue d'enregistrer des informations sur ses utilisateurs après leur déconnexion du service. Selon M. Cubrilovic, lorsque l'utilisateur clique sur le bouton "se déconnecter" de Facebook, le site laisse sur son ordinateur un fichier qui contient des informations personnelles et continue à communiquer à Facebook des éléments sur la navigation de l'internaute.

Pour personnaliser les pages de sites Web, Facebook, comme de nombreux sites ou services, utilise un petit fichier, dit "cookie", déposé sur le disque dur de l'ordinateur, et dans lequel sont stockées des informations sur l'identité et la navigation de l'internaute. Ce fonctionnement est normal : ce qui l'est moins, note M. Cubrilovic, c'est que lorsque l'internaute se déconnecte, le cookie n'est pas effacé, mais simplement modifié. L'utilisateur qui continue à surfer transmet ainsi, sans le savoir, des informations à Facebook ; et le cookie, qui reste sur la machine, conserve des informations à son sujet.

"Si vous vous connectez à Facebook depuis un ordinateur public, et que vous cliquez sur 'se déconnecter'*, vous laissez malgré tout derrière vous des empreintes digitales. D'après ce que je constate, ces empreintes restent présentes jusqu'à ce que quelqu'un supprime manuellement tous les cookies Facebook de l'ordinateur"*, écrit M. Cubrilovic.

En réponse à l'article de M. Cubrilovic, Gregg Stefancik, un ingénieur de Facebook, explique que *"les cookies de Facebook ne sont pas utilisés pour espionner les internautes. Ce n'est tout simplement pas leur rôle. En revanche, nous utilisons ces cookies pour fournir du contenu personnalisé (...), améliorer notre service (...) ou protéger nos utilisateurs et notre service (par exemple pour nous protéger d'attaques par déni de service ou en demandant une deuxième authentification lorsque l'utilisateur se connecte depuis un endroit inhabituel)."*

CONTROVERSES SUR LES NOUVELLES FONCTIONNALITÉS

Google embauche la responsable de la recherche du Pentagone

LEMONDE.FR | 13.03.12 | 14h18

Le logo de la Darpa.Darpa.mil

Regina Dugan, la responsable de la prestigieuse Darpa (Defense advanced research projects agency), le centre de recherche de l'armée américaine, a annoncé qu'elle quittait son poste après trois ans passés à diriger l'institution pour aller travailler chez Google.

Dotée d'un budget de plus de trois milliards de dollars, la Darpa est un organisme très particulier, travaillant sur des projets à court et à très long terme. La Darpa a notamment conçu Arpanet, le précurseur d'Internet, le système GPS, et a conçu les drones Predator couramment employés par l'armée américaine.

Au cours de ses trois années à la tête de l'institution, M^me^ Dugan avait notamment recentré les recherches sur la cybersécurité, en conformité avec les souhaits de l'administration Obama. Elle avait également abandonné certains projets à long terme pour des recherches plus courtes, des choix vus par certains chercheurs comme contraires aux missions de la Darpa. *Wired* rappelle également que M^me^ Dugan fait l'objet d'une enquête administrative portant sur des contrats attribués par la Darpa à une entreprise créée par elle, dont elle est toujours actionnaire.

M^me^ Dugan, qui n'a pas expliqué à quel poste elle travaillerait chez Google, a affirmé qu'elle n'avait pas pu résister à l'envie de travailler pour le moteur de recherche.

Le Monde.fr

Le logo de la Darp

Regina Dugan, la
américaine, a ann

Dotée d'un budget
long terme. La Da
employés par l'arr

Au cours de ses tr
avec les souhaits c
des choix vus par
d'une enquête adr
actionnaire.

M^me^ Dugan, qui n'
le moteur de rech

Le Monde.fr

herche de l'armée
Google.

ts à court et à très
or couramment

curité, en conformité
erches plus courtes,
gan fait l'objet
toujours

vie de travailler pour

ÉDITION ABONNÉS

L'opérateur téléphonique Verizon fournit à la NSA des informations sur des millions d'abonnés

LE MONDE | 06.06.2013 à 15h38 • Mis à jour le 06.06.2013 à 16h12

Par Corine Lesnes

Washington, correspondante. L'administration Bush n'avait pas fait moins. En vertu du Patriot Act et de sa fameuse section 215 qui permet de surveiller les Américains à leur insu, le gouvernement de Barack Obama traque les communications de millions d'abonnés de la compagnie Verizon depuis le 25 avril. Les autorités n'ont pas accès au contenu des conversations, mais peuvent repérer qui parle à qui, d'où et pendant combien de temps.

Cette nouvelle et massive affaire de surveillance téléphonique a fait surface, jeudi 6 juin lorsque le quotidien britannique *The Guardian* a publié sur son site Internet une décision "top secret" du Foreign Intelligence Surveillance Court, le tribunal chargé d'examiner les demandes de surveillance anti-terroriste.

Selon ce document, le juge Roger Vinson a autorisé le FBI (la police fédérale) et la NSA (National Security Agency, l'agence de renseignement militaire, chargée des écoutes électroniques) à réquisitionner pour trois mois les relevés téléphoniques et détails concernant les communications des abonnés du réseau entreprises de

INTERNATIONAL | Mali | Syrie | Corée du Nord | Iran | Planète | Union européenne | Afrique | Amériques | Asie

Numerama

Un hacker confirme les soupçons de traçage de Windows Phone

Simon Robic - publié le Lundi 26 Septembre 2011 à 17h19 - paru dans High-Tech

Actuellement la cible d'une procédure judiciaire, Microsoft pourrait avoir du mal à en sortir vainqueur. Un hacker confirme que Windows Phone envoie des informations de localisation géographique sans le consentement de l'utilisateur, ce que Microsoft a toujours démenti.

Microsoft fait actuellement l'objet d'accusations concernant son système d'exploitation mobile dénommé Windows Phone. Une plainte a même été déposée il y a quelques jours devant la cour fédérale de Seattle. L'OS enverrait régulièrement la localisation géographique de l'utilisateur à *inference.location.live.net* même si ce dernier a refusé d'être localisé par l'appareil.

De son côté, Microsoft dément et a précisé être en train d'enquêter sur ces accusations, en se basant notamment sur les éléments fournis pour déposer la plainte. "*Nous prenons très au sérieux les question de vie privée. Notre objectif était, et est toujours, de fournir aux consommateurs le contrôle sur la façon dont les données utilisées pour déterminer leur localisation sont utilisées, et nous avons développé Windows Phone dans cet esprit*", indique la firme de Redmond.

Cependant, Rafael Rivera, connu pour avoir jailbreaké Windows Phone 7, s'est lui aussi penché sur la question. Il confirme que des paquets sont envoyés à *agps.location.live.net* et à *inference.location.live.net*. Selon ses recherches, les données transmises contiennent la version de l'OS, des informations sur l'appareil et la liste des points d'accès aux alentours (adresses MAC comprises). Ces paquets ont été interceptés au moment où l'appareil a cherché à avoir son approbation pour le faire, et donc avant qu'il accepte. Microsoft pourrait vouloir, en procédant de la sorte, accélérer l'expérience utilisateur. Mais il se demande, donc, si Microsoft conserve ces informations, ou si elles sont simplement supprimées en cas de refus.

Dans tous les cas, cela va à l'encontre de ce que Microsoft annonce pour son système d'exploitation mobile :

- "*Microsoft ne collecte aucune information déterminant la localisation de l'appareil sauf si l'utilisateur a expressément autorisé une application à le faire*"
- "*Microsoft ne collecte que des informations l'aidant à déterminer une localisation approximative de l'appareil si (a) l'utilisateur a autorisé une application à accéder et à utiliser ces données, et (b) si cette application a effectivement demandé l'accès à ces données*".

Affaire à suivre.

Le Monde.fr

NSA (National Security Agency, l'agence de renseignement militaire, chargée des écoutes électroniques) à réquisitionner pour trois mois les relevés téléphoniques et détails concernant les communications des abonnés du réseau entreprises de

Numerama

Le compteur électrique communicant qui étale votre vie privée

Le nouveau compteur électrique Linky d'ERDF a été piraté par un petit groupe de hackers allemands. Ce qu'ils y ont découvert fait un peu froid dans le dos.

Benjamin Gourdet
01net.
le 13/01/12 à 19h50

Le compteur électrique intelligent d'ERDF baptisé Linky en France, ou Smart Meter à l'étranger, a dès sa sortie été l'objet de nombreuses critiques. D'une part, son prix exorbitant (entre 120 et 240 euros) pourrait, malgré l'engagement pris d'ERDF pour une gratuité, être pris en charge par le consommateur.

Par ailleurs, en décembre 2010, l'Agence de l'environnement et de la maîtrise de l'énergie (ADEME) déclarait que « *si le compteur Linky, tel qu'il est actuellement conçu, apporte des bénéfices en termes de comptage et de gestion du réseau électrique, voire de diminution du contenu CO2 du kWh électrique, ses bénéfices pour le consommateur en termes de maîtrise de la demande restent encore théoriques* ». Ce qui a poussé les élus Europe Ecologie/Les Verts de la ville de Paris à rejeter la décision ministérielle d'installation de l'appareil. Enfin, ce sont surtout ses aptitudes à communiquer des données bien plus personnelles que de simples relevés de consommations électriques qui ont fait le plus de remous.

Et c'est précisément sur ce point délicat que nos « pirates technophiles » allemands entrent en scène. En « hackant » le petit boîtier, ils se rendent compte qu'il est capable d'identifier exactement le type et le nombre d'appareils connectés dans votre foyer. Pratique pour automatiser le paiement de la redevance audiovisuelle ! Pire, il peut même savoir précisément la chaîne de télé que vous êtes en train de regarder ! Sur le modèle testé fourni par une société allemande, ils s'aperçoivent que toutes les données transitaient entre le compteur et les serveurs de manière non cryptées.

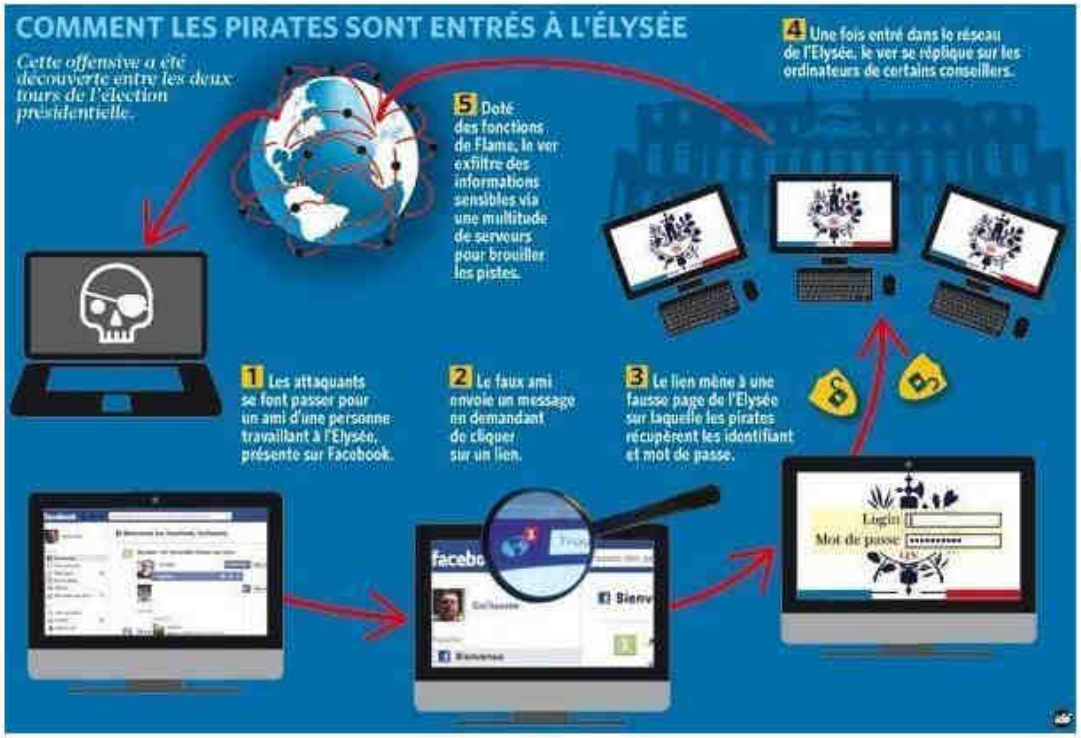
Enfin, poursuivant leurs investigations, ils falsifient les données envoyées à l'aide d'un programme d'émulation, faisant croire que le foyer raccordé au Smart Meter n'avait pas consommé d'électricité pendant deux mois ! Et d'après eux, le piratage de l'appareil est à la portée de tous ou presque, à l'aide de simples outils Windows.

Affaire à suivre.

Le Monde.fr

NSA (National Security Agency, l'agence de renseignement militaire, chargée des écoutes électroniques) à réquisitionner pour trois mois les relevés téléphoniques et détails concernant les communications des abonnés du réseau entreprises de

EXCLUSIF. En mai, l'équipe de Nicolas Sarkozy a été victime d'une opération d'espionnage informatique hypersophistiquée. Les sources de L'Express concordent : le coup vient de... l'ami américain. Révélations sur une attaque qui s'inscrit dans une bataille planétaire.



CYBERGUERRE - Les intrus qui se sont introduits dans les réseaux informatiques de l'Elysée en mai dernier ont subtilisé des notes secrètes et des plans stratégiques à partir des ordinateurs de proches conseillers de Nicolas Sarkozy.
DR

C'est l'un des hold-up les plus audacieux réalisés contre l'Etat français. En mai dernier, quelques jours avant le second tour de l'élection présidentielle, des pirates ont réussi à s'introduire dans les réseaux informatiques de l'Elysée. Révélée par le quotidien régional Le Télégramme, cette intrusion avait alors été soigneusement étouffée par le Château. Une omerta qui, jusqu'à présent, n'avait pas été brisée. Aucune information n'avait filtré sur la nature des agresseurs, ou même sur le préjudice subi. Pourtant, l'affaire est grave, d'autant qu'elle constituerait une cyberattaque sans précédent entre pays alliés.

Sur le même sujet

Cyberattaque contre l'Élysée: la défense de Washington

L'Elysée, victime de deux cyberattaques passées sous silence

Cyberguerre: faut-il craindre les dommages collatéraux?

Recommander 60 Tw

EXCLUSIF. En mai, l'équipe
informatique hypersophistiq
américain. Révélations sur

CYBERGUERRE - Les intrus qui se s
notes secrètes et des plans stratégi
DR

C'est l'un des hold-up les plus
mai dernier, quelques jours ava
des pirates ont réussi à s'intro
l'Elysée. Révélée par le quotidi
avait alors été soigneusement
jusqu'à présent, n'avait pas été
la nature des agresseurs, ou n
est grave, d'autant qu'elle cons
entre pays alliés.

Secret Internet Data-Mining Program

By Victor Luckerson | June 06, 2013 | 31 Comments

Share +1 69 Read Later

One day after The Guardian revealed that the U.S. government has been secretly collecting call log data from millions of Verizon customers, The Washington Post reported Thursday that the government's monitoring of American's data goes much, much deeper. The FBI and the National Security Agency are mining the servers of the country's biggest technology companies for the purpose of hunting spies and terrorists. The program, code-named PRISM, is massive in scope and involves web services that many Americans use every day.

PATRICK SEMANSKY / AP

The National Security Administration campus in Fort Meade, Md., on June 6, 2013.

To make all this shadowy surveillance easier to digest, here are the relevant data points about the massive data collection:

(MORE: 7 Things to Know About the Government's Secret Database of Telephone Data)

Email Print
+ Share Comment
Follow @timenewsfeed

9

The number of tech companies involved in the PRISM program. Here's a list, from an NSA slideshow, including the date when monitoring began:

- Microsoft (September 2007)
- Yahoo (March 2008)
- Google (January 2009)
- Facebook (June 2009)
- PalTalk (December 2009)
- YouTube (September 2010)
- Skype (February 2011)
- AOL (March 2011)
- Apple (October 2012)

dommages collatéraux?

Secret Internet Data-Mining Program

By Victor Luckerson | June 06, 2013 | 31 Comments

Share | +1 69 | Read Later

One day after The Guardian revealed that the U.S. government has been secretly collecting call log data

C'est l'un des hold-up les plus
mai dernier, quelques jours ava
des pirates ont réussi à s'intro
l'Elysée. Révélée par le quotidi
avait alors été soigneusement
jusqu'à présent, n'avait pas été
la nature des agresseurs, ou n
est grave, d'autant qu'elle cons
entre pays alliés.

- Google (January 2009)
- Facebook (June 2009)
- PalTalk (December 2009)
- YouTube (September 2010)
- Skype (February 2011)
- AOL (March 2011)
- Apple (October 2012)

dommages collatéraux?

INTRODUCTION

- Before WWII
  - No export control (1925 Hagelin)
- After WWI
  - Strong export control (Cold war, Rises of terrorism…)
- These controls have always been in place since WWII
- Since 9/11, export controls are strengthened
- In this context, what to think of issues like DES, AES, so-called « crypto freedom », trapdoors, CoCom, Wassenar agreement, Echelon, bitlocker, Carnivore, DCS10000, NarusInsight, Prism…?
- An unsustainable control over Nation States by a handful of States and multinational companies has taken over from the necessary control and protection of each State at the national level (the country, citizens…) by their own!
  - Problem of sovereignty (classical and technological).
  - Security of national companies and interests.

PREREQUISITE

- Without loss of generality, the case of cryptography will be taken as the reccurent theme.
  - The oldest case historycally.
  - The most critical case: who controls cryptography controls everything.
  - The best example for all other IT/security technologies.
- As for all IT/Security technologies, the control over cryptography goes through its implementation and the way it is brought into play:
  - Hardware
  - Software
  - Regulations and standards
  - Commercial power.

CRYPTOGRAPHIC FACTS

- Symmetric cryptography
  - Based on information theory
  - Essentially combinatorial issues prevent any form of actual « provable security »
- Asymmetric cryptography
  - Based on complexity theory
  - No real proof of security until now (is P = NP or not?). Just hope and faith.
- Nowadays the unability to prove an insecurity proof has become a security proof in itself!
  - RSA is secure since no (polynomial time) factoring algorithm has been ever published!

WHAT IS OPERATIONAL CRYPTANALYSIS?

- From an intelligence point of view, breaking an encryption system means
  - Accessing the plaintext in a time shorther than the life of the information (regarding its operational value)
  - Practically speaking: a matter of hours (recall suprecompting time is horribly expensive)
  - With a reduced amount of encrypted data (a few Kb to a few Mb)
  - Must be played a large number of times (a clever enemy changes the key very often)
- These operational constraints mean that academic attacks have just…. an academic interest!
- Mathematical research time vs exploitation time

AIM OF THE TALK

- To present one of the unofficial versions of technology history
- To provide a different reading of cryptology history based on my operational experience
- To explain a few of the issues of « modern cryptology »
- Wlog France and USA will be taken as example of G-20 countries
- Key point: the point of view presented here are answers to my own questions, based on my experience and a number of documents (official, non official, public…)
  - You have to make your own opinion however!
  - Questions are often more interesting than answers!

HISTORY & LEGAL

PREHISTORY: FROM 1945 TO 1975

- Pre-history: from 1945 to 1977 [Cold war Era]
  - Strong need for control of sensitive technologies and information (including computers, GPS, software, telecommunication equipments, electronics, chemistry…)
    - Do not give weapons to the enemy!
    - Export blacklist (CoCom)
  - Deep research in cryptology goes on (originated since 1883) more heavily.
  - Cryptology is considered as military technology
  - Strong export limitation regulations appear (see further)
  - Backdoors are “hardcoded” (Crypto AG and Hans Buehler case; see further)

THE MUTATION PHASE: FROM 1975 TO 2001

- From 1977 to 2001 [End of cold war era; rise of terrorism]
- Classical backdoors are no longer possible. Principle of the "*never put all your eggs in the same basket*".
- Wassenaar agreement (1994) to replace CoCom.
- Socrates project (and 1982 Reagan's discourse on State Union), GATT, WTO, Echelon...
- Academics enter the game. The so-called « modern cryptology » is born
  - Diffie Hellman (1977) & RSA (1978)… 40 years after Bell Labs!
- Freedom for cryptography for everyone [EFF]
  - First clash between worlds [e.g. Gilmore/EFF vs B. Snow/NSA] about Iraq at Crypto'92
- Threat switches to a few communist countries to any world citizen equipped with a computer.

THE GLOBALIZATION PHASE (2001 – 2012)

- Rise of terrorism and of emerging countries (economic terrorism from US perspective ?).
- Multinationals become the new power to serve the strategic dominance and the private sphere is the Nation state new weapon
  - WTO defines the rules. Technology and services are monopoly of a handful (Cisco/Huawei, Microsoft, Google, Facebook, Apple, Intel, RIM…).
- Freedom (until 2004) and then back to control more and more… in a more subtle way!
  - « Cryptographic freedom » results in block cipher hegemony (mostly AES-256) everywhere!
- Standardization of minds (ISO27001 and avatars)
- Rise of computers, computer networks, vulnerabilities (or dynamic intended backdoor?), sophisticated malware, State malware (Magic Lantern, LOPPSI, Bundes Trojan…)
- Rise of the hacker phenomenon (the only existing counterpower nowadays!)

THE LEGAL PHASE: FROM 2012 TO ….

- The last step consist in considering that any citizen is potentially
  - A criminal or a terrorist or both!
  - Mass surveillance transforming democracies into (commercial and political) dictatorships.
- New tools:
  - Intellectual property regulations [PIPA, SOPA, ACTA and equivalent avatars], patent wars (Samsung/Apple, FranceTelecom/Novell…), software patents, war of standards…
  - Licence agreements (read software licences!)
  - Industrial agreements turning into monopolies (Intel/M$ seizure on UEFI…)
  - “Cybercriminality” regulations (UE, Patriot act from evil Bush to Busk-light Obama…)
  - Demonization of hackers (Vupen or CoseInt cases)

One speaking for all others

THE CASE OF CRYPTOLOGY

CRYPTOLOGY CONTROL

- *Who would be so stupid to believe that free, strong and secure cryptography algorithms would be made widely available to anyone without some some of control, especially in the context of cold war, of evergrowing terrorism…?*
- Cryptology is still under a strong control
- http://rechten.uvt.nl/koops/cryptolaw/
- Almost all G-20 countries have a national regulation regarding cryptology (use/export) or at least have signed an international regulation
- Without any control, democraty and citizens' security would be impossible
- The question is: can we accept to sub-contract our cryptographic security to one single nation
  - It must be a national issue, not an international issue (remember Gal de Gaulle)!

THE WASSENAAR AGREEMENT

- http://www.wassenaar.org/
- 42 members
- Cryptology is listed in part 5b
- First level of control:
  - « Good/fair » countries vs other countries (the rest of the world)

FRANCE'S APPLICATION OF WASSENAAR

- Loi n° 2004-575 du 21 juin 2004 pour la confiance en l'économie numérique - Titre III DE LA SÉCURITÉ DANS L'ÉCONOMIE NUMÉRIQUE - Chapitre Ier Moyens et prestations de cryptologie
- Décret n° 2007-663 du 2 mai 2007 pris pour l'application des articles 30, 31 et 36 de la loi n°2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique et relatif aux moyens et prestations de cryptologie
- Décret n° 2001-1192 du 13 décembre 2001 relatif au contrôle à l'exportation, à l'importation et au transfert de biens et technologies à double usage
- Arrêté du 25 mai 2007 définissant la forme et le contenu de déclaration et de demande d'autorisation d'opérations relatives aux moyens et aux prestations de cryptologie
- Règlement (CE) n° 428/2009 du Conseil du 5 mai 2009 instituant un régime communautaire de contrôle des exportations, des transferts, du courtage et du transit de biens à double usage.

PRACTICAL APPLICATION

- G-8 countries are producing cryptographic algorithms
  - National version vs export version
  - Cryptology export control office (in France at Prime Minister level; in USA by NSA; BAWI in Switzerland…)
  - Technical upstream control offices
- National algorithms are for national (classified) use only. No foreign algorithm can be used!
- For NATO countries, very difficult issues to solve (and to maintain) in the context of interoperability.
  - US products and technologies must be used mandatorily (M$, McAfee, Cisco…) by NATO countries!

SECOND LEVEL OF CONTROL

- USA vs the rest of the world
- « *The power of a country lies in its ability to impose standards* »

  Bernard Carayon (French MP)
- US Cryptographic standards everywhere despite the wind of cryptographic freedom!
- During the AES contest, block cipher technology was the only standard authorized (see further)

THIRD LEVEL OF CONTROL

- Use the academic world as a scientific backing
- Academic world has been used as smoke screen and scientific hostage
  - Complexity/combinatorial issues make any real, operational advances in cryptanalysis impossible
  - What is academically broken is far from being broken operationnally
  - Scientific orthodoxy promoted
- Cryptographic algorithms are chosen by the pair {State, Industry} in reality
- About 20 % of cryptology research results only are published (famous example, differential cryptanalysis)

IS THE ACADEMIC COMMUNITY INDEPENDENT?

- I am sorry but the academic community is under some sort of control as well (part of the game)
- Program comitees control
  - Fashion topics « suggested » by higher levels (e.g. Block ciphers, then Hash functions)
  - Clever exploitation of the « publish or perish » effect
- Control by money
  - Research funds (NSF, NSA, FP7…)
- The question is: are you really free to search/publish on any kind of topic?
- Would you authorized to publish real advances in cryptanalysis (e.g. polynomial factoring method)?

CRYPTOGRAPHY INDUSTRY AFTER WWII

- Producing countries of crypto:
  - UK (Racal), D (Siemens), S (Ericsson), CH (Gretag, Crypto AG), FR (Sagem, Thales, Matra), SF (Nokia), H…
  - Guess which is missing?
- In Switzerland, Crypto AG/Greatag hold more than 90 % of the market (since 1945)
  - Almost all countries/organizations (120 in 1995) were buying cryptomachines for {gvt, mil, diplo,economic} needs except a very few (even Vatican ☺)
- 1995 The Hans Buehler case changed the cryptologic face of the world.

The Hans Buehler Case

- Crypto AG's top marketing representative arrested in Teheran in 1992.
- Leaks in the Press (Berlin Club bombing, Chapur Bakhtiar assination in Paris) by Govt officials that gave hints to Iranian government that cryptography was probably trapdoored.
- 9 months in Iranian jails
- Reveals the scandal: NSA, BND and others have infiltrated Crypto AG. Gretag and others to put trapdoors in export versions of cryptomachines systematically
- Crypto AG example of trapdoor (anonymised example from the late 80s)
- The USA were able to read openly most of the world encrypted traffic during nearly 45 years
- Consequences: confidence in cryptography industry is severely weakened
- Need for more « transparency »
  - Next step prepared from the end of the 60s
  - The academic community will be used to play the role of moral/scientific caution
- **Interesting point**: from the early 90s a significant number of trapdoored algorithms were block ciphers!

Lose your illusions

THE BLOCK CIPHER MYSTIFICATION

ACTUAL HISTORY

- Mid 60s the concept of Feistel network is born (IBM & NSA)
- 1971 – Lucifer at IBM
- 1973 – Official birth of block ciphers (Feistel's paper in Scientific American)
- 1973 – DES contest (one candidate, one winner)
  - Lucifer becomes DES under NSA requests
  - First symmetric algorithm published ever by a Nation state… in the context of cold war!
- 1976 – Data Encryption Standard
- End of 60s (declassified 1994) – Russian Gost

DATA ENCRYPTION STANDARD

- Used almost everywhere (nota: still in use!)
  - Swift, authentication mechanisms…
  - Very limited use in the USA
- In fact, the actual standard was not DES but block cipher technology
- Since DES block cipher technology has invaded {information/system/network} security world
- For sensitive traffics, block cipher technology as it is known is not used!

BLOCK CIPHER TECHNOLOGY

- Not really new technology. Self-synchronizing, cipher feeback stream ciphers known from the end of 50s and used for sensitive traffics.
- Very sensitive to channel noise (avalanche criteria effect)
- Emulate stream ciphers but with much overhead compared to real stream ciphers
- No real security proof except « *not publicly broken* = *secure* »
- Once again the scientific community has been manipulated as scientific caution

BLOCK CIPHER TECHNOLOGY (CONTD)

- The reuse of the key from block to block is a major weakness
- You can transform the cryptanalysis problem to a decoding problem… once you have identified a bias/flow or you know a trapdoor
- Provable security is a myth. How model/study 2^{256} sets/functions of 2^{256} blocks (AES 256)?
  - You cannot deal with all combinatorial aspects, all mask values, all characteristics…(combinatorial nightmare)

1992 – KEY YEAR

- Publication of Differential cryptanalysis (DF) by E. Biham
- All block ciphers inspired by DES have been more or less efficiently broken
- DES has not been broken surprisingly
- NSA recognized that it knew DF for 20 years (officially).
- Remark: 1992 – 20 = 1972!

AES CONTEST

- 1997 .- Organized by NIST with the scientific/operational support of NSA
- Rijndael was the winner. From an operational point of view
  - Neither the best… nor the worse
- The key point was to impose a block cipher technology!

A Few Hints

HOW TO HIDE TRAPDOOR

CONTEXT

- Hiding trapdoor is possible as long as the attacker (the author of the trapdoor) has a technological/scientific/legal advantage
- Hence the technology of trapdoors is defined by the scientific/technology context
  - Evolves with the context (computing power, scientific level, size of the academic and/or hacker community…)
- You have to forecast as much as possible what will/can be the evolution 20, 50, 100 years later
  - For computing power, it is relatively easy to forecast
  - For mathematical research it is a little bit more difficult, except if you control/organize research to your benefit.
- The hacker dimension is a new problem: difficult to forecast and model

PRE-HISTORY: FROM 1945 TO 1977

- No academic community
- Algorithms in hardware not in software (crypto devices)
- Not publishing the design was sufficient
- Technical documentations provided mathematically obfuscated description of the algorithm only
- The Crypto AG case.

MODERN CRYPTOLOGY: 1977 - NOW

- Reverse-engineering techniques
  - Software (IDA Pro)
  - Hardware (Starbug/Nohl, Mifare & others)
- Hacking & reconstruction techniques (S. Munaut on Thuraya)
- Keeping cryptographic design secret is non sense!

MODERN CRYPTOLOGY: 1977 – NOW (CONTD)

- Hide trapdoors in protocols' upper layer
  - RC4/Wep? GSM? TCP/IP?...
- And eventually claim for developpers' mistake/incompetence when identified/exploited
  - Industry used as another protection screen
- Vulnerabilities are ideal backdoor since they change regurlarly!
- Exploit users' misuse (reuse of the key)
  - Office encryption (up to M$ Office 2003)?
- Hackers/academics are able to detect most of them
- Use sophisticated malware and dynamic (system level) trapdoor (CanSecWest 2011).

MODERN CRYPTOLOGY: 1977 – NOW (CONTD)

- In most cases, forensics aspects enable to retrieve the secret key very quickly (in RAM, HD)
  - But you need to have access to the computer and/or the application
  - How to manage encrypted traffics (wiretapping/eavesdropping)?
- One solution is key escrowing (RIM/Blackberry)
- The other solution is mathematical trapdoors (one to tie them up all!)
- Statistical testing: standardization of minds
  - FIPS 140 and NIST STS has become THE testing standard
  - Easy to bypass (test simulability). A few countries have developped their own (secret) statistical testing methods

DESIGN TRANSFORMATION

- Consider a secret « starting » algebra A in which you design your algorithm with trapdoor E_T
- Use a oneway transformation S from A to the Boolean algebra $\mathbb{F}_2$
  - Computing $E = S(E_T)$ is computationally easy.
  - Computing E_T from E is computationally untractable
  - E exhibits all desirable cryptographic properties
  - The trapdoor can be detected/used only in A
- Many interesting PhD research topics! ☺
- DeBlock Projet about to be launched in 2013 (financial support pending) in my lab!
  - Combinatorial trapdoor framework for block cipher.

CONCLUSION

CONCLUSION

- We cannot keep stuck on naive/angelic views
- IT/Security technologies (design, products…) should remain a strategic, national issue!
  - Do not lose our national scientific capability
  - Keep away from scientific orthodoxy and « scientific standards »
  - Every country should have a strong, independent academic community working with the State and the Industry
- International/academic standards are neither a fatality nor a doom!
- Being very pessimistic about the scientific community independence and ability, the hacker community is likely/bound to be the new dimension for Nation States
  - Developing and maintaining a large hacker community must become a national issue and strategy!

CONCLUSION: HOW TO RESIST

- The future and the power must be in citizens' hands.
- You will have to choose between your liberty and your security
- Stop to succumb to commercial sirens (Google, Apple, M$...)
  - http://www.prism-break.org
  - Use Linux, Firefox, Thunderbird, Exalead or Yaci…
- The future will be what you want it to be:

It is not a technical issue but a society issue

Thanks you for listening

QUESTIONS & ANSWERS

BIBLIOGRAPHY

- The paper corresponding to this talk is available here
  - http://www.clubdesvigilants.com/archives/2013/02/la-face-cachee-de-la-securite-informatique-ou-les-dessous-dinternet/ (in French)
  - ECIW 2013 Paper https://docs.google.com/viewer?a=v&pid=sites&srcid=ZGVmYXVsdGRvbWFpbnxlcmljZmlsaW9sfGd4OjYxZjM2OWNhYmFjOTQ3ZWQ (with a detailed bibliography)