Ecoutes lors de réunions sensibles : risques et contremesures

JSSI 2018, Paris

Ary Kokos

EY
Building a better working world

Introduction

- **Ecoutes clandestines ou interception : un besoin légitime de se protéger**
  - Réunions sensibles, comités de direction, secret industriel et professionnel (avocat, négociations, etc.)
- **Impossibilité d'empêcher une écoute**
  - Un attaquant décidé trouvera toujours un moyen d'accéder aux communications
  - Exemple d'interception d'échange de hauts dirigeants européens malgré un travail intense de contre intelligence [DE-INT]
- **Mais il est possible de mitiger le risque ou à minima d'augmenter le coût de l'attaque**
- **Objectif: panorama de quelques méthodes d'attaque et mesures pour réduire ce risque**
  - Non exhaustif
  - Focus sur la confidentialité et non l'anonymat
  - Focus sur les mesures techniques liées aux SI et électroniques – autres aspects en particulier de contre intelligence volontairement non traités

Agenda

- **1. Communications entrantes et sortantes**
- **2. « Nettoyage » de la pièce**
- **3. Canaux cachés**
- **4. Limites et aspects de contre surveillance**
- **Conclusion**

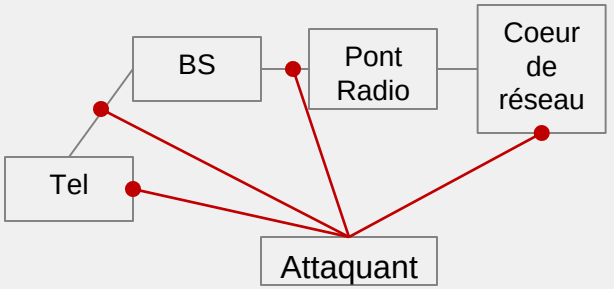
- **Ary Kokos**
- Consultant en sécurité
- EY Genève
- Membre de l'OSSIR

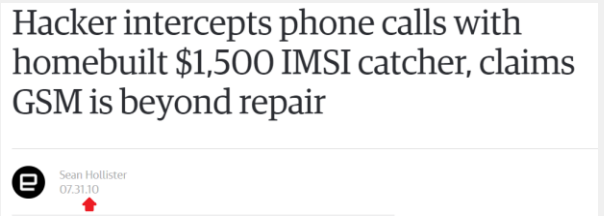
Un grand merci à Jean-Luc Lotti et Ayoub Elaassal

01 Communications entrantes et sortantes

Sécuriser les communications entrantes et sortantes

- **Toutes communications entrantes et sortantes de la salle de réunion peuvent faire l'objet d'une interception**
  - Téléphone, Skype, Visio Conférence, etc.
- **Exemple du cas de communications téléphoniques (une logique similaire peut être adaptée aux autres canaux)**
  - **Au niveau du canal de communications**
    - Lien radio local entre le téléphone et la station de base
    - Lien entre la station de base et le cœur du réseau
    - Au niveau du réseau opérateur
  - **Au niveau des endpoints**
    - Sur les appareils eux même (téléphone)
    - Ou de tout autre objet ou personne situé dans la pièce où a lieu la communication
- **Outre les attaques gouvernementales**
  - Dispositifs locaux d'interception tels que les IMSI catchers accessibles à un détective privé (entre 5 000 $ et 500 000$ au marché noir ou réalisable pour 1 500$ par une personne avec des capacités techniques [IMSI])
  - Logiciels espions à installer sur le téléphone de la cible, accessible pour 150-300 $ par an (écoute, micro d'ambiance, récupération de chat, etc.) [FX]




Hacker intercepts phone calls with homebuilt $1,500 IMSI catcher, claims GSM is beyond repair

Sean Hollister
07.31.10

Sécuriser les communications entrantes et sortantes

- Attaque de cœur de réseau : revue de presse OPERATION SOCIALISTE

When communications are sent across networks in encrypted format, it makes it much harder for the spies to intercept and make sense of emails, phone calls, text messages, internet chats, and browsing sessions. For GCHQ, there was a simple solution. The agency decided that, where possible, it would find ways to hack into communication networks to grab traffic *before* it's encrypted.

The British spies identified Belgacom as a top target to be infiltrated. The

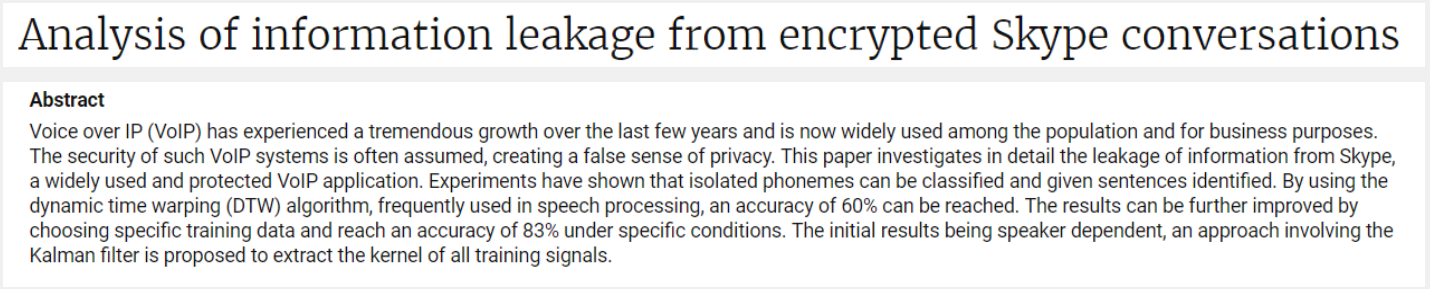
Top-secret GCHQ documents name three male Belgacom engineers who were identified as targets to attack. *The Intercept* has confirmed the identities of the men, and contacted each of them prior to the publication of this story; all three declined comment and requested that their identities not be disclosed.

GCHQ monitored the browsing habits of the engineers, and geared up to enter the most important and sensitive phase of the secret operation. The agency planned to perform a so-called "Quantum Insert" attack, which involves redirecting people targeted for surveillance to a malicious website that infects their computers with malware at a lightning pace. In

Source: [OP-SOC]

Sécuriser les communications entrantes et sortantes

- **Contre-mesure: chiffrement des communications**
  - Usage d'un outil de téléphonie chiffrante : Signal, VoIP sur IPSEC ou même WhatsApp
  - Permet de se prémunir d'une interception réseau classique
- **Limitations**
  - Défaut de conception de l'outil : fuite de métadonnées, analyse d'enveloppe [Skype]*, absence de chiffrement de bout en bout, mauvaise qualité des mécanismes cryptographiques, etc.
    - En France : https://www.ssi.gouv.fr/administration/produits-certifies/



Analysis of information leakage from encrypted Skype conversations

Abstract

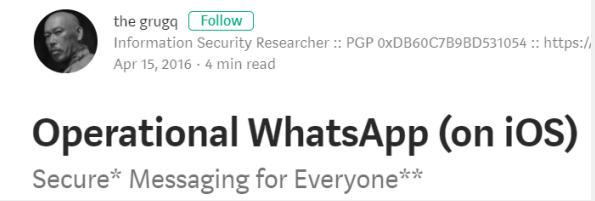
Voice over IP (VoIP) has experienced a tremendous growth over the last few years and is now widely used among the population and for business purposes. The security of such VoIP systems is often assumed, creating a false sense of privacy. This paper investigates in detail the leakage of information from Skype, a widely used and protected VoIP application. Experiments have shown that isolated phonemes can be classified and given sentences identified. By using the dynamic time warping (DTW) algorithm, frequently used in speech processing, an accuracy of 60% can be reached. The results can be further improved by choosing specific training data and reach an accuracy of 83% under specific conditions. The initial results being speaker dependent, an approach involving the Kalman filter is proposed to extract the kernel of all training signals.

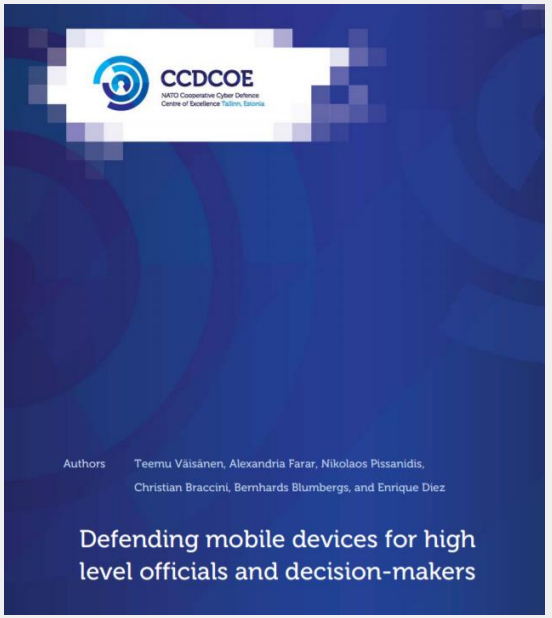
  - Infection du terminal : infection au niveau de trafic, MMS [StageFright], en attaquant le baseband, accès physique, etc.
- **Possibilités d'utiliser des crypto phones dédiés [CS]**
  - Selon les modèles un niveau de sécurité supérieur contre certains vecteurs d'inoculation (mais pas toujours)
  - Tout en considérant d'une part que ce système est potentiellement backdooré - l'important étant plus de choisir par qui
  - Et qu'il est peu probable qu'il puisse résister à une attaque d'une agence de renseignement compétente : vulnérabilité, implant matériel, etc
- **Ou implémenter un système sur mesure** – voir les spécifications Commercial Solutions for Classified Program de la [NSA]

*Note: Skype supporte un chiffrement de bout ne bout depuis le début de l'année [Skype E2E]

Sécuriser les communications entrantes et sortantes

- **Defending mobile devices for high level officials and decision-makers du NATO Cooperative Cyber Defence Centre of Excellence [CCDOE]**
- **Ou quelques conseils pour des particuliers du Grugq [WH]**



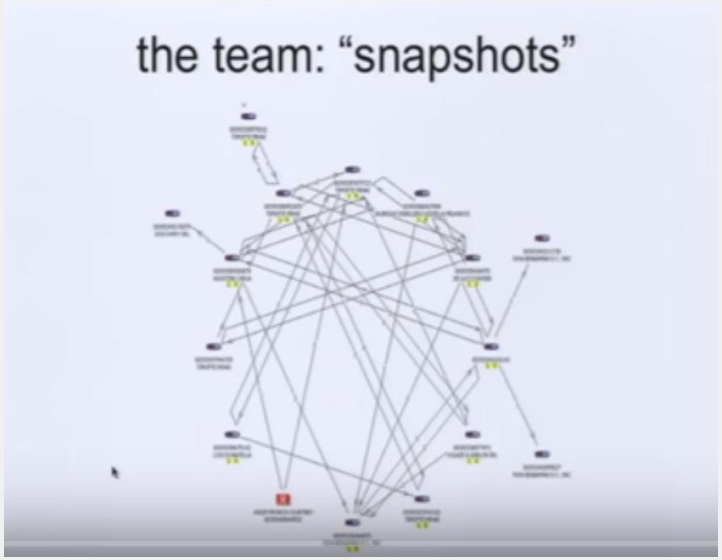


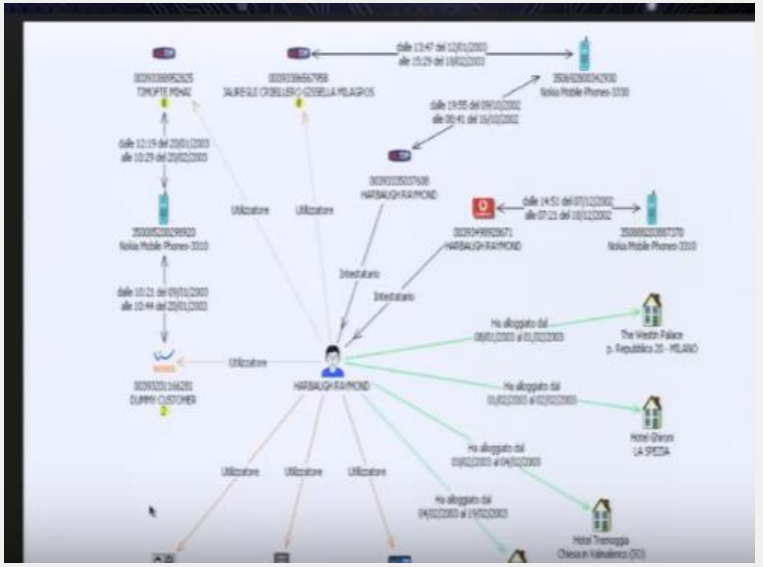
- **Importance de définir la cible de sécurité / l'appétit au risque**
  - Contre qui et quoi l'entreprise veut elle se défendre ?
    - Mesures différentes si on considère un employé mécontent, un détective privé ou une agence étatique (police locale, agence de renseignement d'un pays peu développé ou NSA ?)
  - Equilibre entre sécurité et usage
    - cf cas de VIP n'utilisant pas leur téléphone chiffrant

- Note : L'usage de téléphone prépayé ou pris sous un faux nom n'est pas non plus une solution, l'attaquant pouvant écouter toutes les communications dans un périmètre ou procéder par reconnaissance vocale ou analyse des métadonnées pour identifier sa cible (par exemple 2 téléphones se déplaçant toujours en même temps, etc.)

Sécuriser les communications entrantes et sortantes

- Black Hat USA 2013 - OPSEC failures of spies [BH]
  - “In 2005, news organizations around the world reported that an Italian court had signed arrest warrants for 26 Americans in connection with an extraordinary rendition of a Muslim cleric. At the heart of the case was the stunning lack of OPSEC the team of spies used while they surveilled and then snatched their target off the streets of Milan.”



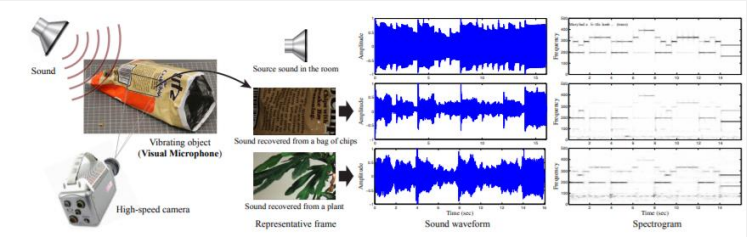


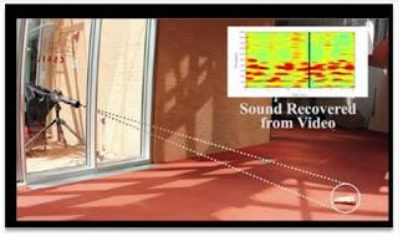
02 «Nettoyage» de la pièce

«Nettoyage» de la pièce

- **Avant même de considérer les dispositifs d'écoute clandestins insérés dans la pièce…**
  - Il est nécessaire d'éliminer tous les dispositifs d'enregistrement : téléphones, smartwatches, enregistreurs, MP3, pendentifs connectés, etc.
  - Cf exemples précédents des logiciels espions sont accessibles au grand public ou vendus par des entreprises telles que Hacking Team ou Gamma ou encore un usage personnel de certains outils par des membres des forces de l'ordre [300]

- **Attention aux hauts parleurs et caméras**
  - Un haut parleur fonctionne sur le même principe qu'un microphone et les dispositifs de sonorisation de la pièce peuvent être modifiés
  - Caméras permettant de lire sur les lèvres ou tout simplement le support de présentation
- **Tourner la caméra n'est pas toujours suffisant**
  - une vidéo des vibrations produites par la voix sur un objet de la pièce peuvent être utilisées pour reconstituer le son (feuille, emballage) voir étude du [MIT Vidéo et Paper]





«Nettoyage» de la pièce

- **Sans oublier le rétroprojecteur**
  - Attaque pour récupérer les images
  - Backdoor de systèmes de diffusion par USB
  - Ou implant électronique dans le câble (voir le projet RAGEMASTER de la NSA dont le coût serait de 30$) [ANT]

TOP SECRET//COMINT//REL TO USA, FVEY

RAGEMASTER

ANT Product Data

(TS//SI//REL TO USA,FVEY) RF retro-reflector that provides an enhanced radar cross-section for VAGRANT collection. It's concealed in a standard computer video graphics array (VGA) cable between the video card and video monitor. It's typically installed in the ferrite on the video cable.

24 Jul 2008

(U) Capabilities

(TS//SI//REL TO USA,FVEY) RAGEMASTER provides a target for RF flooding and allows for easier collection of the VAGRANT video signal. The current RAGEMASTER unit taps the red video line on the VGA cable. It was found that, empirically, this provides the best video return and cleanest readout of the monitor contents.

(U) Concept of Operation

(TS//SI//REL TO USA,FVEY) The RAGEMASTER taps the red video line between the video card within the desktop unit and the computer monitor, typically an LCD. When the RAGEMASTER is illuminated by a radar unit, the illuminating signal is modulated with the red video information. This information is re-radiated, where it is picked up at the radar, demodulated, and passed onto the processing unit, such as a LFS-2 and an external monitor, NIGHTWATCH, GOTHAM, or (in the future) VIEWPLATE. The processor recreates the horizontal and vertical sync of the targeted monitor, thus allowing TAO personnel to see what is displayed on the targeted monitor.

Unit Cost: $ 30

«Nettoyage» de la pièce

- **Nettoyage de la pièce à la recherche d'implants**
  - Contenu tiré de l'excellente présentation de M. Glasser et J Prusan [BlackHat]

- **Inspection visuelle**
  - Un premier contrôle mais de loin insuffisant : des microphones peuvent être cachés dans des objets (stylos, meubles, etc.) ou dans la masse des murs (au moment de la construction ou a posteriori)

- **Analyseur de spectre**
  - Utile pour détecter les systèmes d'émissions rudimentaires
  - Mais plus compliqué d'identifier les systèmes d'émission en rafale ou transmettant après l'inspection
  - Ou encore si des fréquences «normales» dans le contexte sont utilisées (GSM, Wifi)

- **Autres approches possibles (non exhaustif)**
  - Analyse des réflexion du signal
  - Localisation d'émission radio
  - Utilisation d'un détecteur de jonction non linéaire (permet de détecter la présence de semi-conducteurs et donc particulièrement utile pour l'inspection des murs, sols ou objets comme des tables)
  - Rayons X pour les objets

«Nettoyage» de la pièce

- **Focus : Détecteur de jonction non linéaire et «babble tapes»**

Détecteur de jonction non linéaire [HK]

10. Special Inspection Activities (used only as needed)
Non Linear Junction Detector (NLJD) inspection - active and passive
X-ray, radiographic, and fluoroscope inspection
Magnetic anomaly inspection

11.Preventive Actions (available only by special request)
Seal and dust all cavities, wall plates, artifacts, etc...
Install acoustic, ultrasonic, IR, and RF "cloak" as needed
Install IPM alarms and associated security system
Installation of encryption devices
Installation of high security locks, doors, and hinges
Installation of physical security devices
Client education and training

Extrait de la présentation de Glasser et Prusan

- **Sur le terrain il est compliqué de demander à des VIP de se soumettre à ce type d'inspections et souvent le mieux qui puisse être demandé est de déposer leurs dispositifs électroniques à l'entrée**

03 Canaux cachés

Canaux cachés

- **Propagation des ondes sonores**
  - Lieux spécialement conçus pour propager les ondes sonores (risque plus particulièrement présent dans les lieux non maîtrisés tels que les hôtels, centres de congrès, etc.)
  - Note : selon certains documents ayant fuité le GCHQ (agence britannique) aurait mis en place un système de surveillance des réservations d'hôtel afin de rediriger les cibles vers des lieux plus adaptés pour les écoutes [GCHQ]


UK TOP SECRET STRAP1

ROYAL CONCIERGE

A SIGINT driven hotel reservation tip-off service

From: reservations@expensivehotel.com
To: new-target@mod.gov.xx

"Thank you for reserving....."

ROYAL CONCIERGE exploits these messages and sends out daily alerts to analysts working on governmental hard targets

What hotel are they visiting?
Is it SIGINT friendly?

An enabler for effects – can we influence the hotel choice? Can we cancel their visit?

We can use this as an enabler for HUMINT and Close Access Technical Operations

An excerpt from a top secret GCHQ document from the archive of NSA whistleblower Edward Snowden.

  - Ou encore monter un amplificateur de son sur un petit drone amené autour du lieu de rendez vous au dernier moment

Salle "Bruxelles" ou nous sommes actuellement : enregistrement des sons

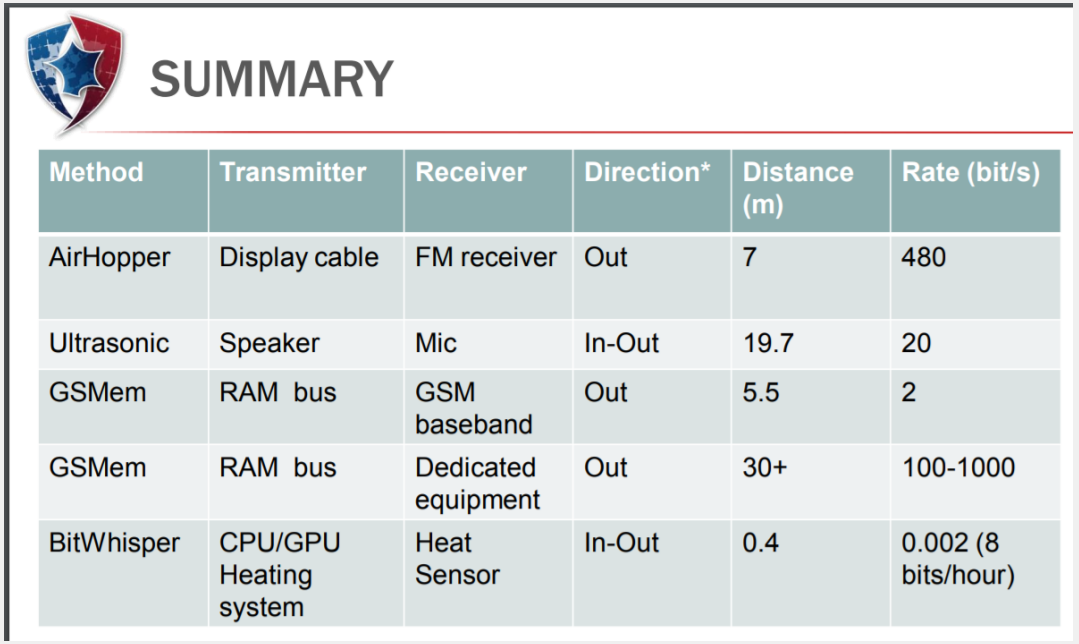
Canaux cachés

- Fuites électromagnétiques (Tempest) : écran, claviers, câbles, etc.
- Selon les cas, l'usage d'une cage de Faraday peut être nécessaire
- Ou en déplacement une tente de Farady [US], qui au delà des ondes, diminue aussi le risque lié aux caméras

President Obama with members of his team in a mobile war room in a tent

Canaux cachés

- Sans oublier tous les canaux cachés possibles : lumineux, thermiques, vibrations, etc.
  - Voir les travaux de M. Guri [GURI] [GURI2] et de l'ANSSI [ANSSI BOTCONF]



SUMMARY

Method	Transmitter	Receiver	Direction*	Distance (m)	Rate (bit/s)
AirHopper	Display cable	FM receiver	Out	7	480
Ultrasonic	Speaker	Mic	In-Out	19.7	20
GSMem	RAM bus	GSM baseband	Out	5.5	2
GSMem	RAM bus	Dedicated equipment	Out	30+	100-1000
BitWhisper	CPU/GPU Heating system	Heat Sensor	In-Out	0.4	0.002 (8 bits/hour)

04 Limites et aspects de contre surveillance

Limites et aspects de contre surveillance

- **Contre-mesures classiques**
  - Changement de lieu
  - Analyse de la menace
  - Etc.

- **Attaquer les attaquants**
  - Une surveillance active est d'une part elle-même vulnérable à une contre surveillance (les équipes d'attaque n'étant pas toujours formées elles même à la contre surveillance, ce en particulier dans le cas d'individus plus amateurs)
  - En ayant connaissance de cette surveillance, il est possible de manipuler l'attaquant / exploitation du biais de l'excès de confiance dans les mesures électroniques
    - Ex : cas terroriste Moyen-Orient ayant laissé son téléphone à un tiers opérant un trafic normal pendant qu'il était en Europe
  - Attention : la surveillance peut elle-même être constituée de deux équipes, une servant de pot de miel/appât alors qu'une seconde plus entrainée est également présente mais de façon plus discrète

Limites et aspects de contre surveillance

- **Limites**
  - Humaines : corruption, manipulation de personnes présentes
  - Bêtise : débriefing de la réunion avec un conjoint, scan des notes manuscrites sur le MFP non protégé
- **Difficultés d'identifier des acteurs compétents sur le marché**
  - Lorsque le contexte le permet, contacter les services de l'Etat
- **Processus**
  - Le niveau de sécurité doit être maintenu en permanence
  - Ex : une inspection annuelle de la salle du conseil laisse une période vulnérable très large

Conclusion

Conclusion

- **Que faire pour se protéger**
  - Premièrement prendre conscience du risque
  - Etablir sa cible de sécurité et son appétit au risque
  - Définir un niveau réaliste de sécurité
    - Rien ne sert de donner un téléphone chiffrant à un VIP s'il est tellement compliqué à utiliser qu'il préfère passer par son téléphone personnel

- **Pour un niveau de base**
  - Signal ou logiciel similaire
  - Exclure tous les dispositifs électroniques de la pièce
  - Pour certaines informations hautement confidentielles écrire sur des morceaux de papier pliés

- **Dans les cas plus sensibles**
  - Consulter des personnes ayant les bonnes compétences
  - Note : si vous êtes la cible d'une menace étatique il vous faudra très probablement le support d'une entité étatique

Autres référence

Présentation basée sur un article précédemment publié de l'auteur [AK]

Blog du Grugq [GGQ]

How to pwn phones with shady replacement parts [RR]

DoD DMCC-S [DMCC]

TSG Standards [TSG]

Revue de presse de la première page

http://www.lemonde.fr/pixels/article/2015/07/01/en-allemagne-la-nsa-a-surveille-les-communications-de-merkel-et-de-nombreux-ministres_4666535_4408996.html ;

https://www.nouvelobs.com/politique/20140305.OBS8533/ce-que-disent-les-enregistrements-de-patrick-buisson.html

http://www.lepoint.fr/actualites-societe/2008-09-30/l-affaire-des-ecoutes-de-l-elysee-definitivement-close/920/0/278356

http://www.lemonde.fr/pixels/article/2015/03/31/que-sont-les-imsi-catchers-ces-valises-qui-espionnent-les-telephones-portables_4605827_4408996.html

EY | Assurance | Tax | Transactions | Advisory

Le contenu de cette présentation présente l'avis de l'auteur qui n'est pas nécessairement celui d'EY.