Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

S . G . D . S . N
Agence nationale de la sécurité des systèmes d'information
CERT-FR

Paris, le 06 juin 2017
N° CERTFR-2017-ACT-023

Affaire suivie par :
CERT-FR

BULLETIN D'ACTUALITÉ

Objet : Bulletin d'actualité CERTFR-2017-ACT-023

1 - Ultrasons et ordiphones

Fin avril, lors de la conférence EuroS&P (IEEE European Symposium on Security and Privacy), des chercheurs ont présenté un papier intitulé « Privacy Threats through Ultrasonic Side Channels on Mobile Devices » [1] dans lequel ils s'intéressent à l'utilisation qui est faite des ultrasons pour localiser un ordiphone.

Fréquences audibles et ordiphones

Pour rappel, le spectre des fréquences audibles par un humain est compris entre environ 20 Hz et 20 kHz (sons graves et aigus, respectivement). Ce spectre dépend de chaque individu, les aigus étant moins bien perçus avec l'âge notamment. Lorsqu'une fréquence trop élevée pour être audible par l'oreille humaine est utilisée, on parle d'ultrason.

Si la plupart des personnes ne sont pas capables de percevoir des sons au-dessus de 18 kHz, notamment lorsqu'ils sont intégrés à d'autres sons (une musique par exemple), la plupart des ordiphones peuvent eux capter des sons jusqu'à 20 kHz.

Impact sur la vie privée

Le papier s'intéresse à l'exploitation de cette situation par certaines entreprises pour suivre les habitudes d'utilisateurs. Celles-ci procèdent de la manière ci-dessous :

- émission de balises ultrasonores (*ultrasound beacons*) dans des magasins, lors d'évènements ou dans des émissions de télévision ;
- intégration d'un algorithme dans des applications pour ordiphones pour analyser les fréquences reçues par le microphone.

Selon les entreprises, divers mécanismes de modulation et algorithmes sont utilisés pour rendre les sons le moins audibles possible et détecter les erreurs de transmission (cf. sections 5.1 et 5.2 du papier).

Autres impacts

Ce papier s'ajoute à la liste des publications de plus en plus fréquentes ([2] par exemple) concernant l'emploi des ultrasons et des ordiphones, que ce soit :

- pour suivre les habitudes d'utilisateurs comme détaillées ci-dessus ;
- pour identifier l'ensemble des équipements informatiques utilisés par une personne, à des fins marketing ou pour trouver l'identité d'une personne utilisant un mécanisme d'anonymisation tel que Tor sur son ordinateur ;
- pour appairer des appareils entre eux ;
- pour exfiltrer des données d'un système sensible protégé par un mécanisme d'*air gap*.

Conclusion

L'utilisation de techniques basées sur la réception d'ultrasons par les ordiphones semble de plus en plus courante, mais n'est pas toujours désirée. Pour s'en prémunir, plusieurs pistes peuvent être suivies :

- paramétrer les permissions de l'ordiphone pour n'autoriser que les applications de confiance à accéder au microphone ;
- si un magasin d'applications géré par l'organisation est utilisé, vérifier l'absence d'algorithme d'analyse d'ultrason au sein de l'application avant de l'ajouter au magasin (cf. section 4.3 du papier) ;
- ne pas connecter d'haut-parleurs à un système sensible et de ne pas utiliser d'équipements non contrôlés à proximité d'un système sensible [3].

Documentation

1. Privacy Threats through Ultrasonic Side Channels on Mobile Devices
   http://christian.wressnegger.info/content/projects/sidechannels/2017-eurosp.pdf
2. Schedule 33. Chaos Communication Congress
   https://fahrplan.events.ccc.de/congress/2016/Fahrplan/events/8336.html et media.ccc.de - Talking Behind Your Back
   https://media.ccc.de/v/33c3-8336-talking_behind_your_back
3. Instruction interministérielle relative aux systèmes traitant des informations classifiées de défense de niveau confidentiel-défense
   https://www.ssi.gouv.fr/uploads/2015/04/II920-janv2005.pdf

2 - Rappel des avis émis

Dans la période du 29 au 05 juin 2017, le CERT-FR a émis les publications suivantes :

- CERTFR-2017-AVI-166 : Multiples vulnérabilités dans SCADA les produits Siemens

Durant la même période, les publications suivantes ont été mises à jour :

- CERTFR-2017-ALE-008 : Multiples vulnérabilités dans Microsoft Windows XP et Windows Server 2003 (ajout d'une mesure de contournement pour le code d'attaque ESTEEMAUDIT affectant le protocole RDP.)

Gestion détaillée du document

06 juin 2017 version initiale.