REDOCS

Rencontre Entreprises DOCtorants en Sécurité

O. Blazy & **P. Lafourcade**

LIMOS — Université Clermont Auvergne

Journées Nationales, Juin 2022

cnrs GDR Groupement de recherche **Sécurité Informatique**

Rencontres Entreprises DOCtorants en Sécurité

REDOCS



REDOCS 2022, 7ème édition

Pour les doctorants

- Découvrir des problèmatiques industrielles
- Étudier de nouveaux sujets
- Travailler en équipe
- Tisser des liens

Pour les entreprises

- Identifier des problèmatiques de recherche
- Avoir un regard académique
- Présentation d'idées originales
- Trouver de nouveaux collaborateurs

Entreprises 20 = 4 + 4 + 3 + 3 + 3 +3


AIRBUS

CRYPTO EXPERTS

Quarkslab
SECURING EVERY BIT OF YOUR DATA

AMOSSYS

MINISTÈRE DES ARMÉES

gemalto
security to be free

THALES
Together • Safer • Everywhere

Worldline

UBISOFT

EDF

THALES
Together • Safer • Everywhere

SystemX
INSTITUT DE RECHERCHE TECHNOLOGIQUE

Qwant

beys

facebook

CNIL.
COMMISSION NATIONALE
INFORMATIQUE & LIBERTÉS

orange™

REDOCS

Doctorants 91 = 15 + 15 + 15 + 15 + 15 + 16

REDOCS

Edition 2022 :

Date : 28 novembre au 3 décembre 2022

Lieu: CIRM à Luminy



Inscriptions : `redocs-org@irisa.fr`

- CV académique
- email d'autorisation du directeur de thèse

\+ prise en charge du déplacement

REDOCS

Sujets REDOCS'22

Entreprises :

Sujets :

- Développer un protocole d'authentification sécurisé.
- Réalisation de signatures comportementales pour détecter des logiciels malveillants impactant le système de fichiers.
  Analyse de sécurité de composants matériels
- Inventer une méthode automatique pour générer un jeu d'entrées fournissant une couverture d'arêtes à 100% pour des parseurs de certificats X.509.

`https://gdr-securite.irisa.fr/redocs`

REDOCS

Conclusion

https://gdr-securite.irisa.fr/redocs

Les sujets sont en ligne

Les inscriptions sont ouvertes

Recherche de doctorants

Recherche d'entreprises pour REDOCS'23

Témoignage d'Anais Barthoulot,
REDOCS'21 au CIRM,
sujet de la CNIL

REDOCS

Merci pour votre attention!

Questions?

https://gdr-securite.irisa.fr/redocs

redocs-org@irisa.fr

REDOCS

Risques des objets connectés sur la vie privée

Anaïs Barthoulot, Daniel De Almeida Braga,
Diane Leblanc-Albarel, Gwendal Patat, Morgane Vollmer

June 24, 2022

Our team

- Daniel: Cryptographie dans la Nature : La Sécurité des Implémentations et Standards Cryptographiques
- Diane: Distribution de compromis temps-mémoire cryptanalytique
- Gwendal: Briser la confiance : exploration des implementations de la TrustZone ARM sur les smartphones
- Morgane: Support logiciel en représentation modulaire des nombres pour le chiffrement homomorphe sur processeurs parallèles
- Anaïs: Chiffrement avancé pour le partage de données sensibles

REDOCS

Our team

- Daniel: Cryptographie dans la Nature : La Sécurité des Implémentations et Standards Cryptographiques
- Diane: Distribution de compromis temps-mémoire cryptanalytique
- Gwendal: Briser la confiance : exploration des implementations de la TrustZone ARM sur les smartphones
- Morgane: Support logiciel en représentation modulaire des nombres pour le chiffrement homomorphe sur processeurs parallèles
- Anaïs: Chiffrement avancé pour le partage de données sensibles

REDOCS

Our team

- Daniel: Cryptographie dans la Nature : La Sécurité des Implémentations et Standards Cryptographiques
- Diane: Distribution de compromis temps-mémoire cryptanalytique
- Gwendal: Briser la confiance : exploration des implementations de la TrustZone ARM sur les smartphones
- Morgane: Support logiciel en représentation modulaire des nombres pour le chiffrement homomorphe sur processeurs parallèles
- Anaïs: Chiffrement avancé pour le partage de données sensibles

REDOCS

Our team

- Daniel: Cryptographie dans la Nature : La Sécurité des Implémentations et Standards Cryptographiques
- Diane: Distribution de compromis temps-mémoire cryptanalytique
- Gwendal: Briser la confiance : exploration des implementations de la TrustZone ARM sur les smartphones
- Morgane: Support logiciel en représentation modulaire des nombres pour le chiffrement homomorphe sur processeurs parallèles
- Anaïs: Chiffrement avancé pour le partage de données sensibles

REDOCS

Our team

- Daniel: Cryptographie dans la Nature : La Sécurité des Implémentations et Standards Cryptographiques
- Diane: Distribution de compromis temps-mémoire cryptanalytique
- Gwendal: Briser la confiance : exploration des implementations de la TrustZone ARM sur les smartphones
- Morgane: Support logiciel en représentation modulaire des nombres pour le chiffrement homomorphe sur processeurs parallèles
- Anaïs: Chiffrement avancé pour le partage de données sensibles

REDOCS

Subject

Testing protection of users' private life by everyday connected objects

Aim: searching practical attacks on several connected objects, following the unboxing and PIA methodologies

REDOCS

Outline

REDOCS

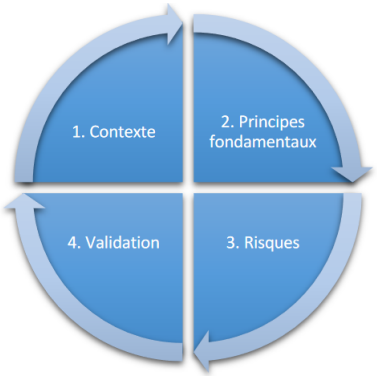
Methodologies

- **Unboxing**: as if the object was used for the first time
- **PIA**: Privacy Impact Assessment and/or Data Protection Impact Assessment

REDOCS

Methodologies

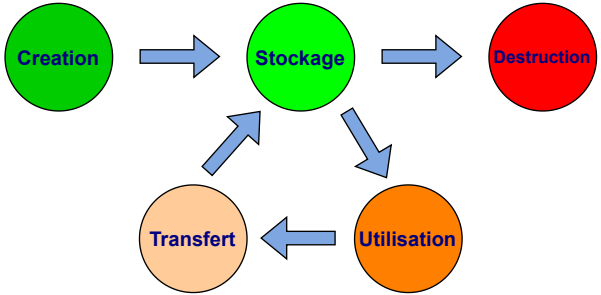
- **Unboxing**: as if the object was used for the first time
- **PIA**: Privacy Impact Assessment and/or Data Protection Impact Assessment



REDOCS

PIA

- Context:
  - Outline of the processing: nature, scope, context, purposes and stakes
  - Data, processes and supporting assets:



PIA

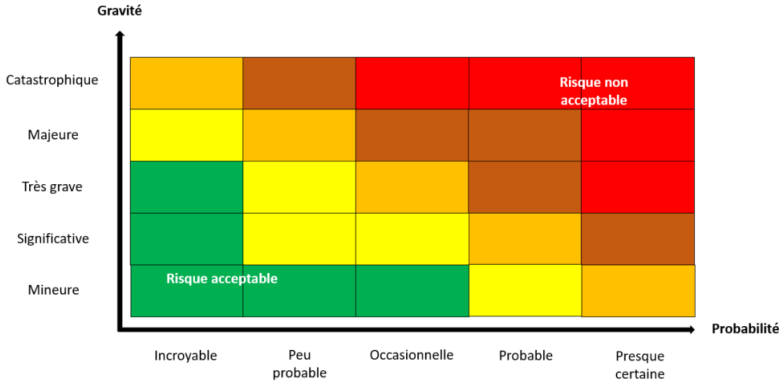
- Context:
  - Outline of the processing: nature, scope, context, purposes and stakes
  - Data, processes and supporting assets:

- Fundamental principles:
  - Regardless of the nature, severity and likelihood of risks
  - Established by law (GDPR)
  - Must be respected

REDOCS

PIA

- Risks and evaluation:



Suggested objects

- 10 suggested objects
- 6 chosen, including
  - two USB adapter devices
  - toy for children
  - connected alarm clock

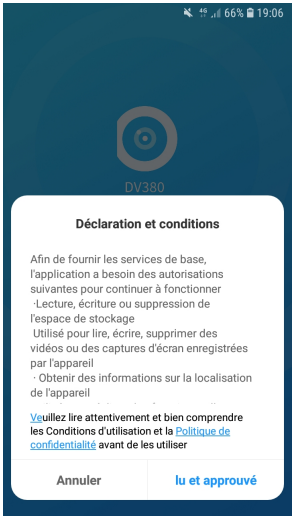
REDOCS

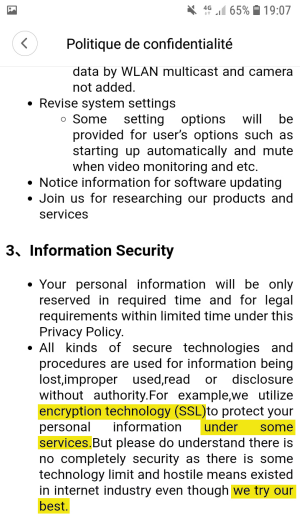
Outline

REDOCS

Aim: provide USB adapter and domestic surveillance.

Documentation





Identified threats

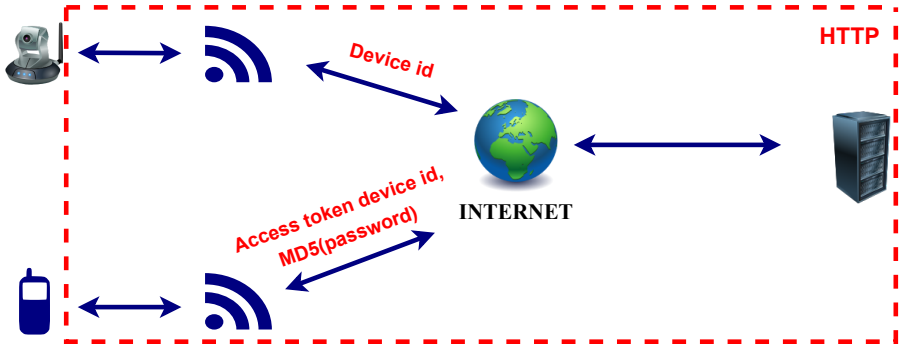
Impacts potentiels
Divulgation d'images
Dénis de service
Perte des vidéos

Sources
Source humaine externe
Source non humaine

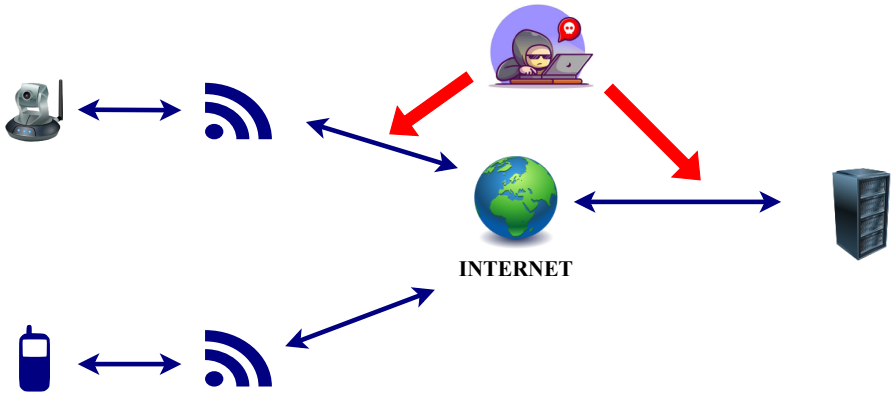
Menaces
Ecoute sur le wifi
Brute force
Ecoute sur internet
Effacement de la carte SD

REDOCS

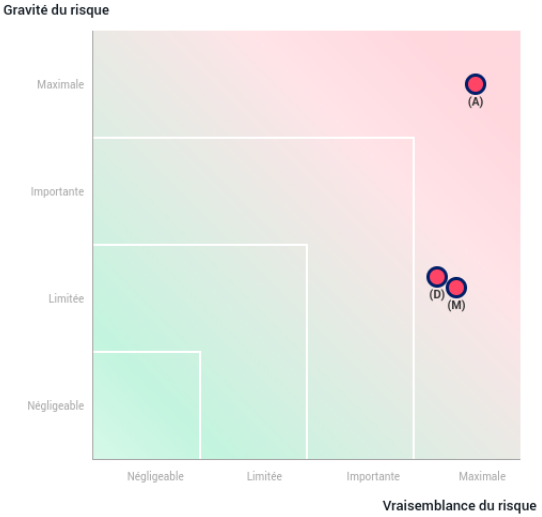
Network analysis



Description of the attack



Final evaluation



- Illegitimate (A)ccess to data
- Unwanted (M)odification of data
- (D)isappearance of data

Outline

REDOCS

Official purpose: Provide a user friendly, secure and adapted phone for kids.

REDOCS

Documentation

traitement des données à caractère personnel peut inclure Hong Kong, la Chine, et les États-Unis.

Durée de conservation : Aussi longtemps que la personne utilise un compte dans le cadre de nos services ou pendant 2 semaines à compter de la demande d'effacement faite par la personne.

Données : Nom et adresse, Adresse électronique, Données nécessaires pour fournir le service, Données générées pendant le service, Carte d'identité ou copie de passeport.

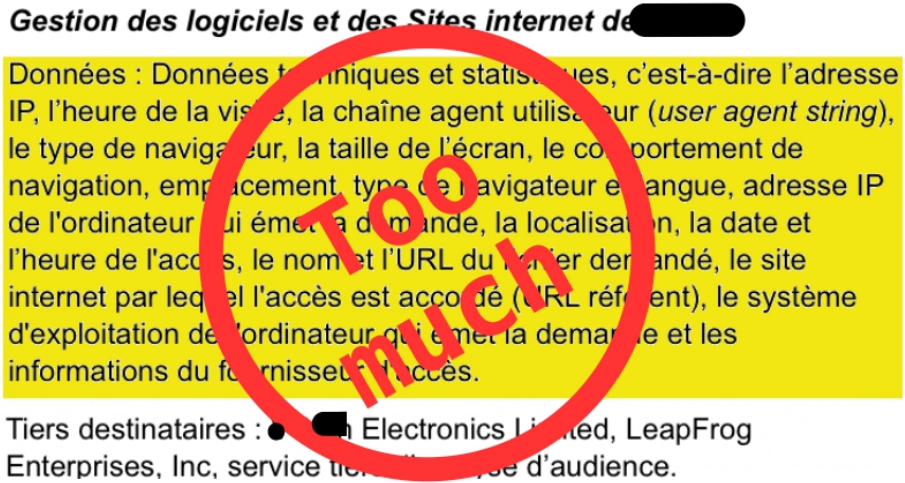
Documentation

Gestion des logiciels et des Sites internet de

Données : Données techniques et statistiques, c'est-à-dire l'adresse IP, l'heure de la visite, la chaîne agent utilisateur (*user agent string*), le type de navigateur, la taille de l'écran, le comportement de navigation, emplacement, type de navigateur et langue, adresse IP de l'ordinateur qui émet la demande, la localisation, la date et l'heure de l'accès, le nom et l'URL du fichier demandé, le site internet par lequel l'accès est accordé (URL référent), le système d'exploitation de l'ordinateur qui émet la demande et les informations du fournisseur d'accès.

Tiers destinataires : Electronics Limited, LeapFrog Enterprises, Inc, service tiers d'analyse d'audience.

Documentation



Gestion des logiciels et des Sites internet de [redacted]

Données : Données techniques et statistiques, c'est-à-dire l'adresse IP, l'heure de la visite, la chaîne agent utilisateur (*user agent string*), le type de navigateur, la taille de l'écran, le comportement de navigation, emplacement, type de navigateur et langue, adresse IP de l'ordinateur qui émet la demande, la localisation, la date et l'heure de l'accès, le nom et l'URL du fichier demandé, le site internet par lequel l'accès est accordé (URL référent), le système d'exploitation de l'ordinateur qui émet la demande et les informations du fournisseur d'accès.

Tiers destinataires : [redacted] Electronics Limited, LeapFrog Enterprises, Inc, service tiers d'analyse d'audience.

Previous threats

CYBERSÉCURITÉ

[redacted] se fait hacker les données de 200 000 enfants.

Par Valentin Blanchot - @vblanchot
Publié le 1 décembre 2015 à 09h48 - Mis à jour le 12 octobre 2017 à 17h36

Security of the device

Identified threats

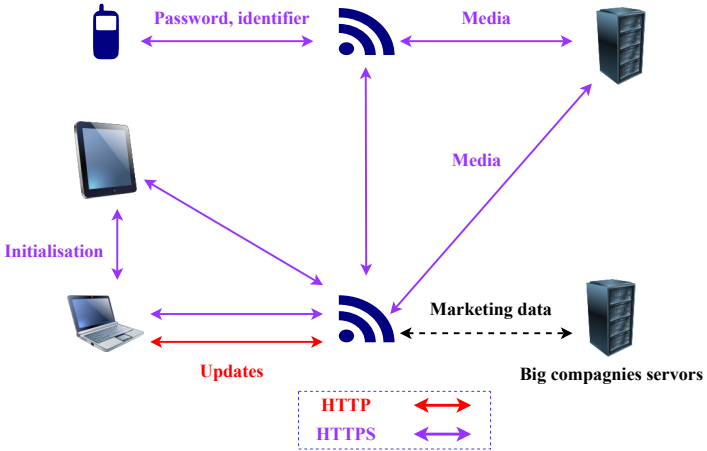
Impacts potentiels
Divulgation/Utilisation d'images
Divulgation de données
Dénis de service
Perte des vidéos
Interactions non sollicitées avec l'enfant
Diffusion de contenu non adapté à l'enfant

Menaces
Ecoute sur le wifi
Ecoute sur le réseau filaire
Effacement de la mémoire

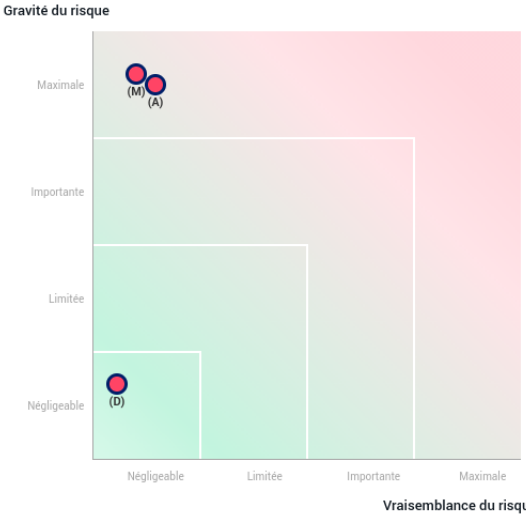
Sources
Source humaine externe
Source humaine interne
Source non humaine

REDOCS

Networking analysis



Final evaluation



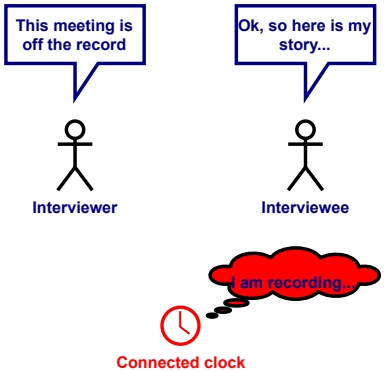
- Illegitimate (A)ccess to data
- Unwanted (M)odification of data
- (D)isappearance of data

Outline

REDOCS

Alarm Clock with a connected speaker: a possible attack

Only the **owner** has agreed to the data policy.



Companion apps

An app can hide another!

Companion apps

An app can hide another!

APP SCORES

LOOK CAM

Average CVSS 6.9

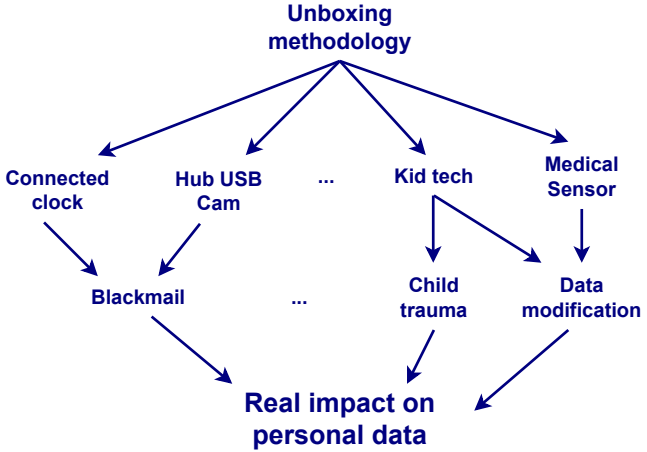
Security Score 10/100

android.permission.READ_PHONE_STATE	dangerous	read phone state and identity
android.permission.RECORD_AUDIO	dangerous	record audio
android.permission.REQUEST_INSTALL_PACKAGES	dangerous	Allows an application to request installing packages.

Outline

REDOCS

Conclusion


Unboxing methodology
Connected clock
Hub USB Cam
...
Kid tech
Medical Sensor
Blackmail
...
Child trauma
Data modification
Real impact on personal data

Thanks for your attention
Any Questions?

@ anais.barthoulot@orange.com
@ daniel.de-almeida-braga@irisa.fr
@ diane.leblanc-albarel@irisa.fr
@ gwendal.patat@irisa.fr
@ morgane.vollmer@univ-brest.fr

Article on: https://linc.cnil.fr/fr/risques-des-objets-connectes-sur-la-vie-privee-lanalyse-de-doctorants-en-securite-redocs

REDOCS