Alexa, tell us a joke!
"Privacy"

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

October 29, 2021

CNIL.
COMMISSION NATIONALE
INFORMATIQUE & LIBERTÉS

- Created in 1978
- Independent administrative authority
- Alert, guidance and information to all public
- Control and sanctions

Subject

Testing protection of users' private life by everyday connected objects

Aim: searching practical attacks on several connected objects, following the PIA methodology

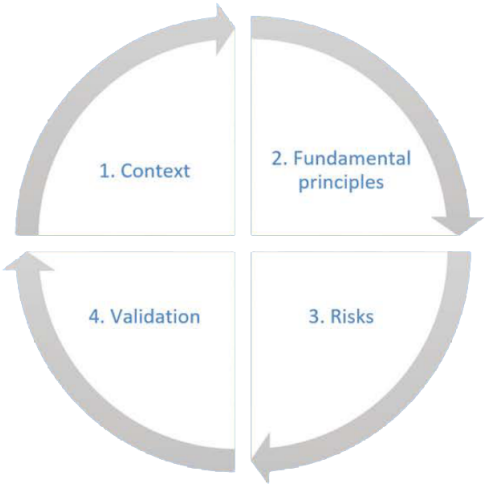
Outline

Privacy Impact Assessment

Privacy: all fundamental rights and freedoms

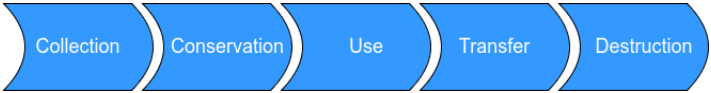
PIA acronym: Privacy Impact Assessment and/or Data Protection Impact Assessment

Privacy Impact Assessment methodology



Context

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



Fundamental principles

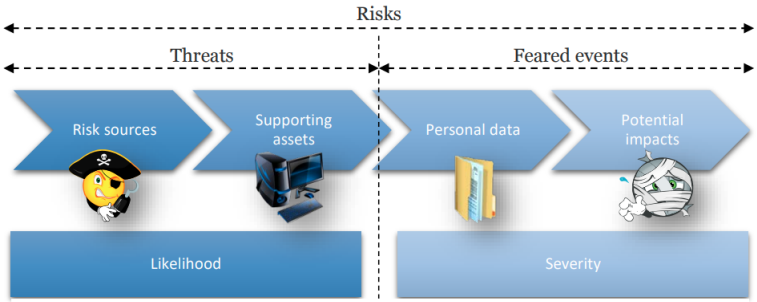
- Fundamental rights and principles
- “Non-negotiable”
- Established by law (GDPR)
- Must be respected
- Regardless of the nature, severity and likelihood of risks

Fundamental principles

- Fundamental rights and principles
- “Non-negotiable”
- Established by law (GDPR)
- Must be respected
- Regardless of the nature, severity and likelihood of risks

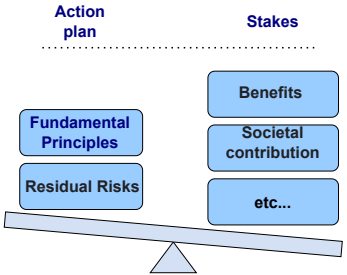
Contract $\neq$ Consent

Risks


Risks
Threats
Feared events
Risk sources
Supporting assets
Personal data
Potential impacts
Likelihood
Severity

Evaluation

- Validated
- Conditional on improvement
- Refused



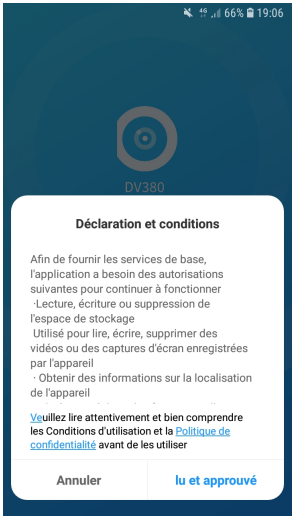
Suggested objects

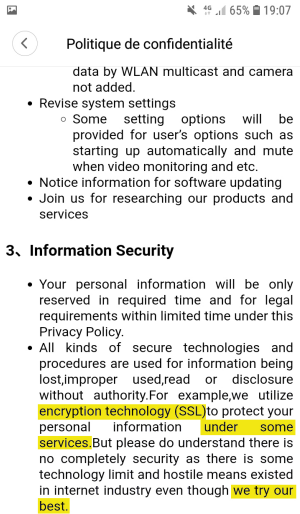
- 10 suggested objects
- 6 chosen, including
  - two USB adapter devices
  - toy for children
  - connected alarm clock

Outline

Aim: provide USB adapter and domestic surveillance.

Documentation





Identified threats

Impacts potentiels

- Divulgation d'images potent...
- Dénis de service
- Perte des vidéos

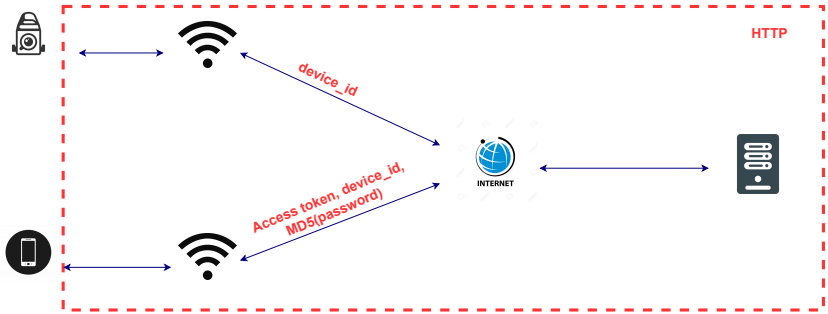
Menaces

- Ecoute sur le wifi
- Brute force
- Ecoute sur Internet
- Effacement de la carte SD

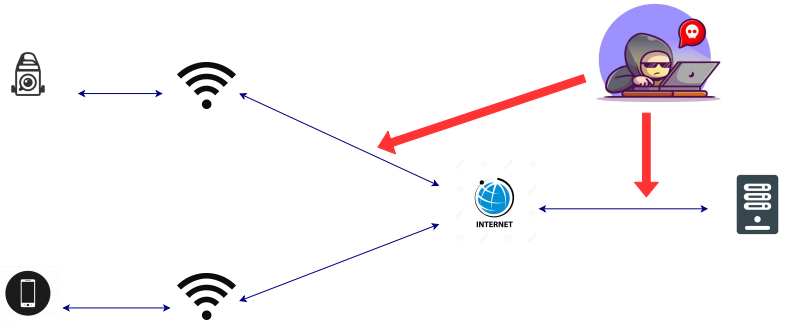
Sources

- Source humaine externe (att...
- Source non humaine (incendi...

Network analysis

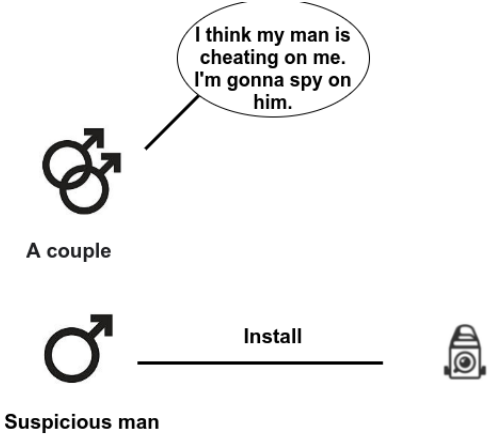


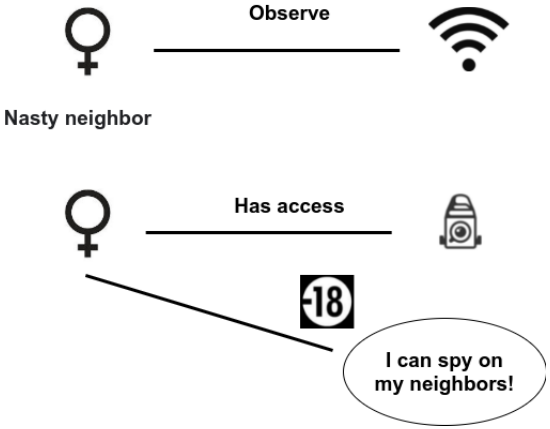
Description of the attack



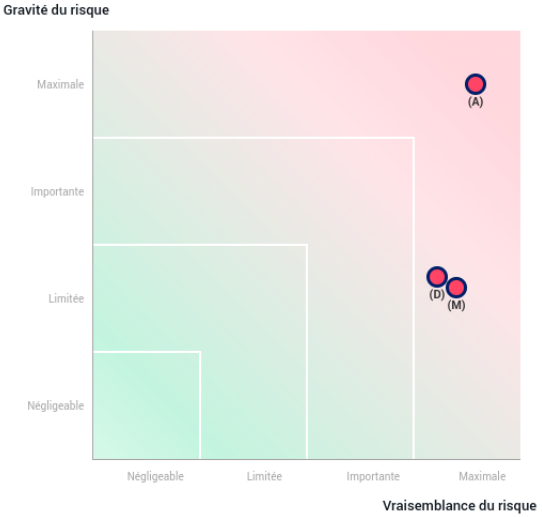
Video of the attack

Attack scenario




Observe
Nasty neighbor
Has access
-18
I can spy on
my neighbors!

Final evaluation



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

Outline

Aim: provide USB adapter and domestic surveillance.

Documentation

NONE

Identified threats

Impacts potentiels

Divulgation d'images potent...
Dénis de service
Perte de vidéos

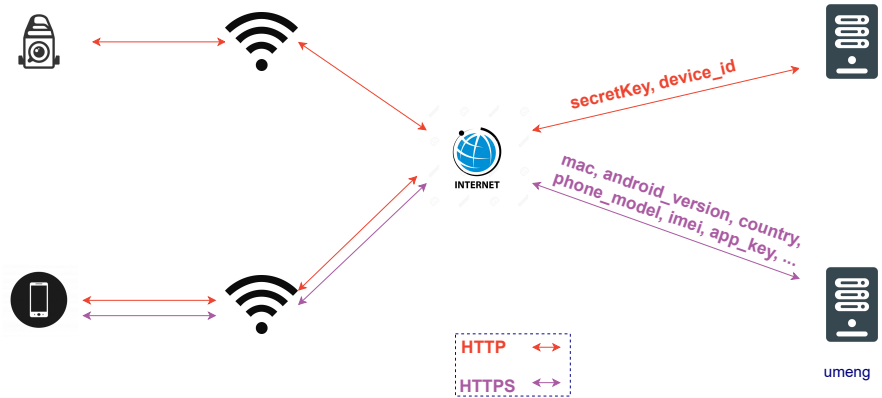
Sources

Source humaine externe (att...
Source non humaine (incendi...

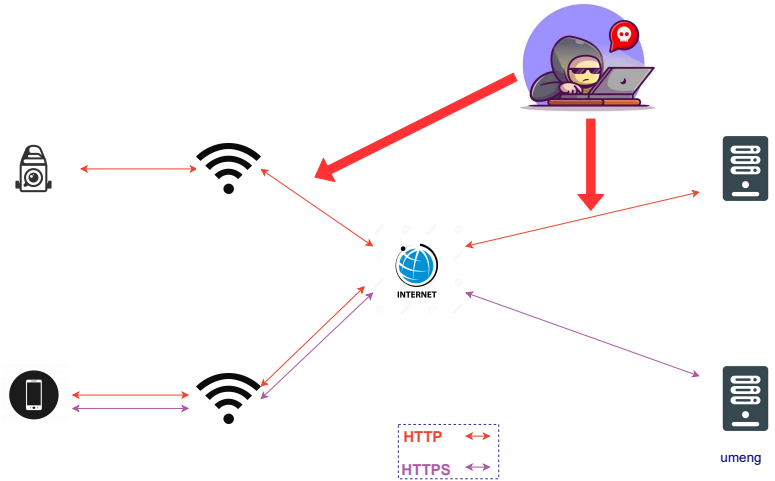
Menaces

Ecoute sur wifi
Brute force
Effacement carte SD

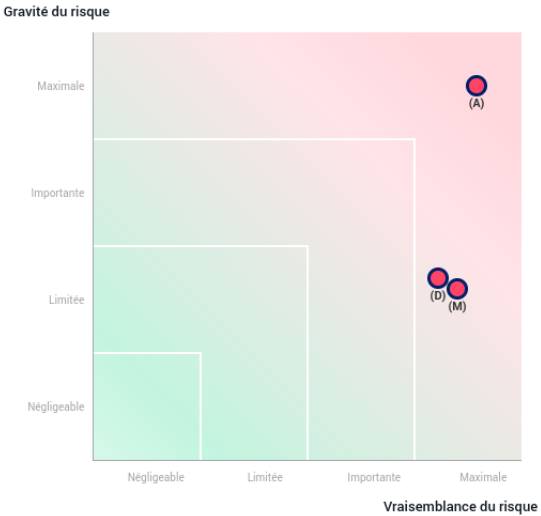
Network analysis



Description of the attack



Final evaluation



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

Outline

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

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.

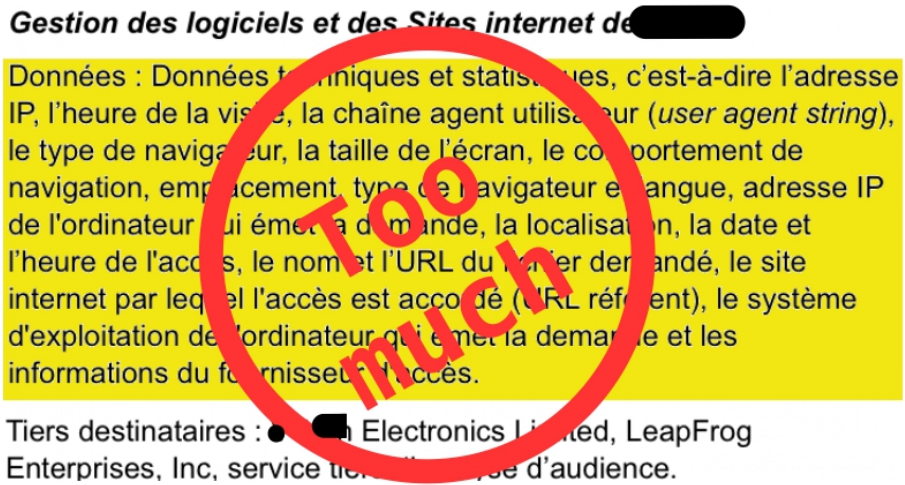
Documentation

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.

Too much

Identified threats

Impacts potentiels

- Divulgation ou utilisation ...
- Interaction non sollicité e...
- Contenu non adapté à l'enfant
- Dénis de service
- Perte de photo/video

Sources

- source humaine externe
- Source non humaine
- Source humaine interne

Menaces

- Ecoute sur le wifi
- Ecoute sur le réseau filaire
- Effacement de la mémoire de...

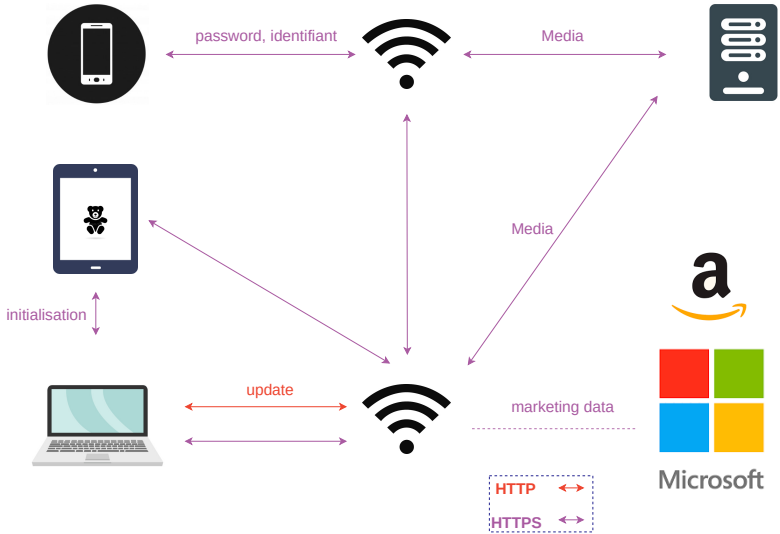
Previous threats

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

Networking analysis

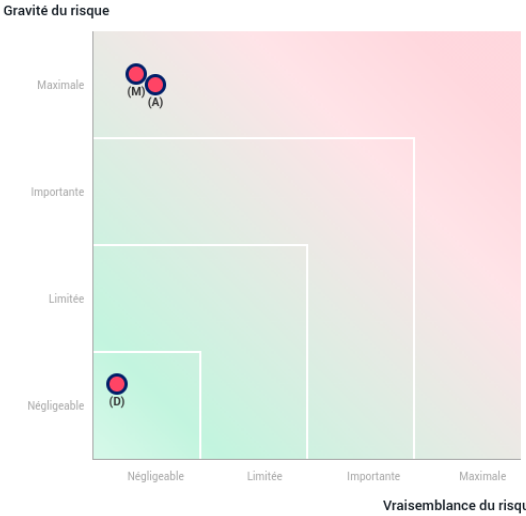


Description of the Attack

- Attack on the password

- Man in the Middle (data interception)

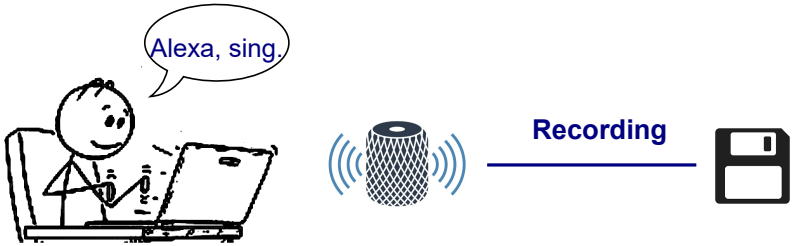
Final evaluation



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

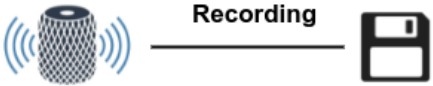
Outline

Alarm Clock with a connected speaker



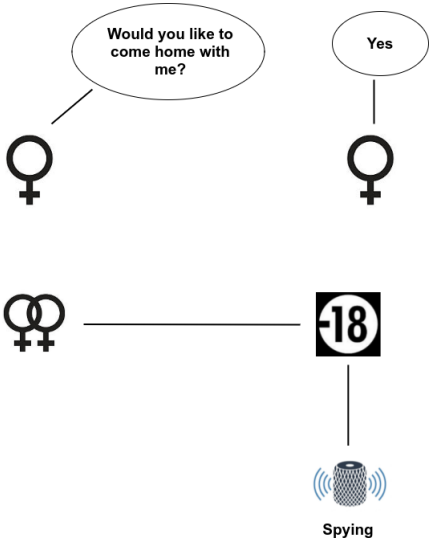
Alarm Clock with a connected speaker

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



An example

A possible attack



Companion apps

An app can hide another!

Companion apps

An app can hide another!

APP SCORES

LOOK CAM

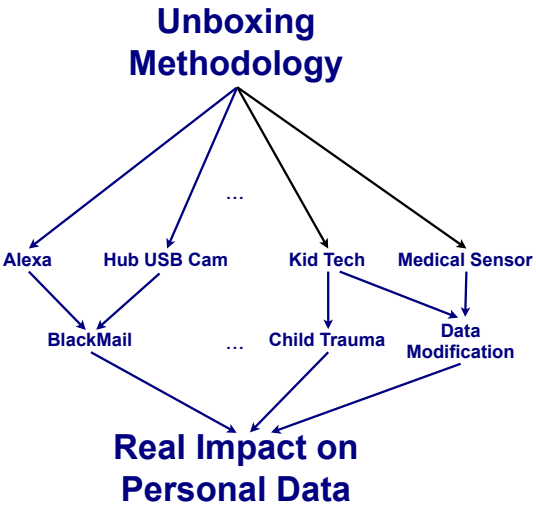
Average CVSS 6.9

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

Conclusion


Unboxing Methodology
...
Alexa
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