

Introduction aux modèles de menaces



Proposition de définition



Une manière de strictement penser au type de protection dont vous avez besoin pour vos données.

Il est impossible de les protéger contre toute sorte de subterfuges ou d'attaquants, vous devez donc vous concentrer sur les personnes susceptibles de vouloir accéder à vos données, ce qu'elles veulent en retirer et la manière de les obtenir.

Élaborer un ensemble d'attaques possibles contre lesquelles vous envisagez de vous protéger se dénomme modèle de menace.



Proposition de définition

Le modèle de menaces peut être représenté sous forme de diagramme en trois sections ;

- les données que vous voulez protéger
- les menaces extérieurs
- les moyens pour protégez vos données

Exemple de profils

- Journaliste
- Blogueur en zone de conflit
- Militant des droits de l'homme
- Lanceur d'alerte
- Citoyen soucieux de défendre sa vie privée
- Ado gay, lesbienne
- Femme d'un mari jaloux, violent
- etc

Blogueur en zone de conflit

Les données à protéger

Article en cours de rédaction, sources, échanges avec les sources...

Menaces extérieurs

Gouvernement, police, armée, terroristes
(risque d'arrestation, de prison, de mort ?)

Moyens pour protégez les données

Chiffrement des données, OS live amnésique, messagerie instantanée chiffrée

Femme d'un mari jaloux

Les données à protéger

Messages personnels, navigation web, sms...

Menaces extérieurs

Mari jaloux, violent ?

Moyens pour protégez les données

Navigation privée, mot de passe sur le smartphone, smsecure...

Ado gay, lesbienne

Les données à protéger

SMS, navigation web

Menaces extérieurs

Parents, connaissances

Moyens pour protégez les données

Navigation privée, TOR, OS amnésique, chiffrement du smartphone

Blogueur en zone de conflit (dictature)

Gouvernement, police

Piratage d'ordinateur,
installation de mouchards,
Piratage de boîte mail,
attaques homme du milieu,
installation de trojans,
surveillance de masse,
récupération de données upstream (NSA)

Terroristes

Recoupement d'informations,
Attaque homme du milieu

Chiffrement des fichiers

Article en cours de rédaction

Messagerie chiffrée

Échanges avec les sources

Os amnésique

Coordonnées des sources

Citoyen soucieux de défendre sa vie privée

Les données à protéger

Données personnelles, mot de passes...

Menaces extérieurs

Gouvernement, police, pirates...

Moyens pour protégez les données

Chiffrement des fichiers, gestionnaire de mots de passe

Citoyen soucieux de défendre sa vie privée

Gouvernement, police

installation de mouchards légaux,
attaques homme du milieu,
surveillance de masse,
récupération de données upstream (NSA),
IMSI catcher,
boites noires...

Voisin curieux

Attaque sur le wifi,
Capture des trames réseau

Chiffrement des fichiers

Messagerie chiffrée

Messagerie chiffrée

Mots de passes robustes
sécurisation de sa box (wifi)

Données privées

Contact avec des militants

Organisation
de manifestations

Ordinateurs personnel,
Tablettes/smartphone,
Documents...

Une démarche globale

La protection de données sensible ne passe pas que par le chiffrement

Défendre sa vie privée est une démarche globale

Exemples

- 👎 Envoyer des sms chiffré dans le métro
- 👎 Envoyer sa clé privée GPG en pièce jointe
- 👎 Faire des mails de masse avec des adresses en copie carbone
- 👎 Laisser un inconnu utiliser sa session avec ses clés privées

Exemples de logiciels

Chiffrement des fichiers

Veracrypt, encfs (Windows) / LUKS, cryptsetup (GNU/Linux)

Gestion des mots de passe

Keepass, KeepassX

Messageries chiffrées

Tox, Cryptochat, MyCryptoChat

OS amnésique

TAILS

Navigateur anonyme

TOR

Tous les logiciels ne sont pas adaptés à toutes les menaces !

Bien se renseigner avant de faire usage d'un logiciel est primordial !

Sources

[Ressources de communication autour des Cafés Vie Privée \(Github\)](#)

[Une Introduction au Modèle de Menace \(EFF\)](#)

Merci de votre attention !

Place aux questions,
et aux ateliers pratiques !