



Étude des attaques associées aux **Vo**ls de Cookies

Cahier des charges

Ouverture à la recherche 2022 - 2023

Encadrants

[BEGIN Thomas](#)

[GELAS Jean-Patrick](#)

Étudiants

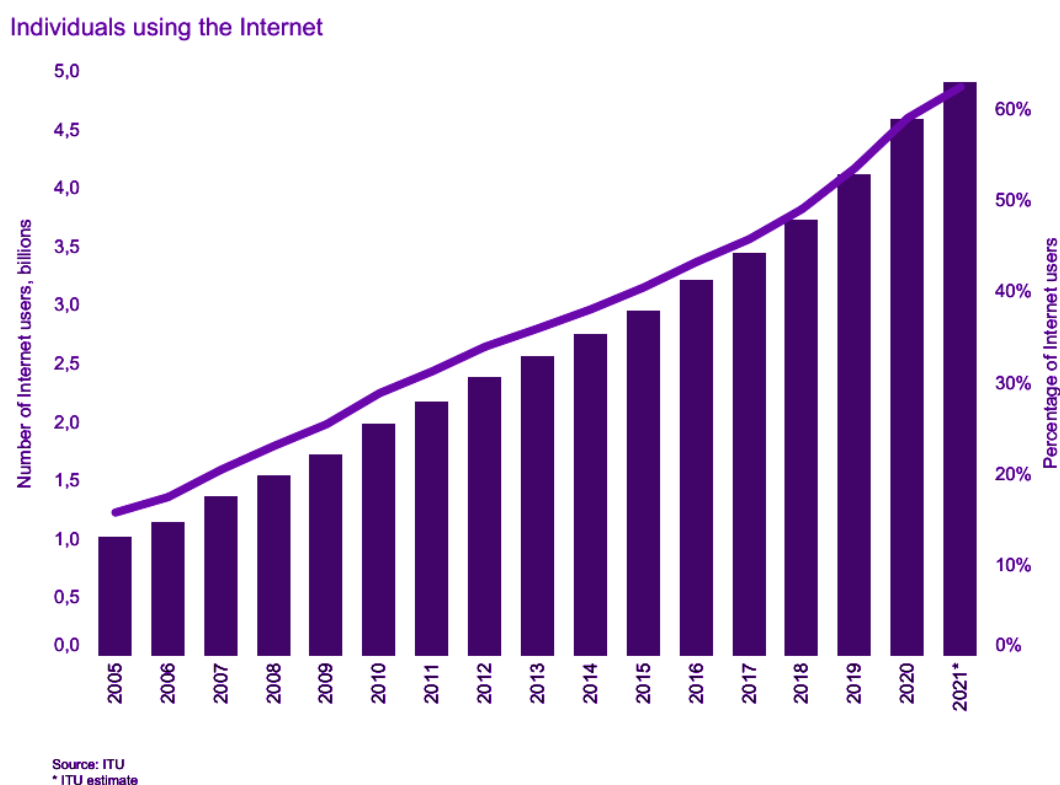
LEDRU Romane

PHANG Roméo



1. Contexte

Internet est depuis longtemps une source d'innombrables possibilités d'apprentissage, de développement professionnel / personnel et de création de valeur. Il est estimé qu'en 2021 nous étions plus de **4,9 Milliards d'utilisateurs*** (Source: itu.int) à travers le monde. Ce carrefour d'informations a permis le développement de plusieurs domaines mais également la créations de certains; notamment la **cybersécurité**.



(Image 1) Évolution du taux d'usages d'Internet de la population - itu.int

L'une des applications les plus utilisées d'internet est le **web**. Celui-ci permet aujourd'hui d'accéder à la majorité de vos services du quotidien via votre **navigateur web**. Au sein du navigateur on peut donc naviguer sur différents sites internet et y **renseigner ou utiliser des données**.



A. Les cookies 🍪 ?

Un cookie est un texte inséré dans votre navigateur pendant la navigation sur le web. Il permet aux différents sites que vous visitez de **conserver des informations** à **votre** sujet, comme vos **données de connexions** ou vos préférences visuelles. Cela permet donc de revisiter par la suite ce site sans avoir à renseigner une nouvelle fois son nom d'utilisateur ou son mot de passe.

B. Cas d'utilisations

Les cookies sont **invisibles** pour l'utilisateur mais restent une composante importante aux sites internet: ils permettent d'améliorer l'expérience utilisateur (cookies strictement nécessaires, cookies de **performance**, cookies de fonctionnalités...), tout comme **tracer** celui-ci afin de mettre en place un marketing ciblé pour des futures autres navigations (cookies de ciblage marketing, cookies inconnus/autres...). L'intérêt est donc une navigation plus fluide pour les utilisateurs et alléger la quantité de données transmises sur le net.

C. Ses faiblesses

Nous allons particulièrement nous pencher sur les **cookies de session**. Comme son nom l'indique, il sert à retrouver vos informations après avoir quitté la page et y être revenu. Il est tout particulièrement **visé par des vols**, pour son contenu (**accès aux données sensibles et personnelles**) et par sa **faible sécurité**.

On observe déjà 3 types d'attaques :

- vol par accès physique à la machine,
- vol par sniffing ou par MITM ([Man-In-The-Middle](#)),
- vol par l'exploitation du navigateur.

2. Objectifs

Dans le cadre de ce projet de recherche, nos principaux axes de développements sont:



A. DIY usurpation d'identité par vol de cookie

Sur ce point nous allons mettre en place un axe de recherche sur **comment appliquer** les différents types d'attaques que nous avons cité dans la partie des faiblesses du cookie. On verra donc comment voler une identité, par **accès physique** dans un premier temps, par **sniffing** et **MITM** dans un second temps puis pour finir par l'exploitation des faiblesses du **navigateur**.

B. Les solutions de mitigations

Après avoir les connaissances nécessaires pour voler une identité ou les données de connexion d'une personne par un vol de cookie, nous allons nous pencher sur les **solutions pour s'en prévenir**.

C. L'étendue des impacts

Pour finir les recherches, nous ferons un bilan sur les **impacts** que ces attaques peuvent avoir. Nous nous pencherons sur les différents niveaux et **degrés de danger atteignable** en fonction de facteurs, tels que **le type** ou **la taille** de la victime / infrastructure, etc.

D. Conception d'un TP pour les M2

Dans le cadre de ce projet de recherche, nous serons aussi amenés à créer un **TP** sur les différentes attaques par vols de cookie, pour un niveau **Master 2**.

3. Réalisations

Liste non exhaustive des réalisations attendues pour notre projet de recherche :

- Cahier des charges,
- Rapport intermédiaire,
- Rapport final,
- TP pour les Master 2,
- Soutenance,
- Vidéo de vulgarisation (optionnel).



4. Délais et répartitions

Répartition du travail

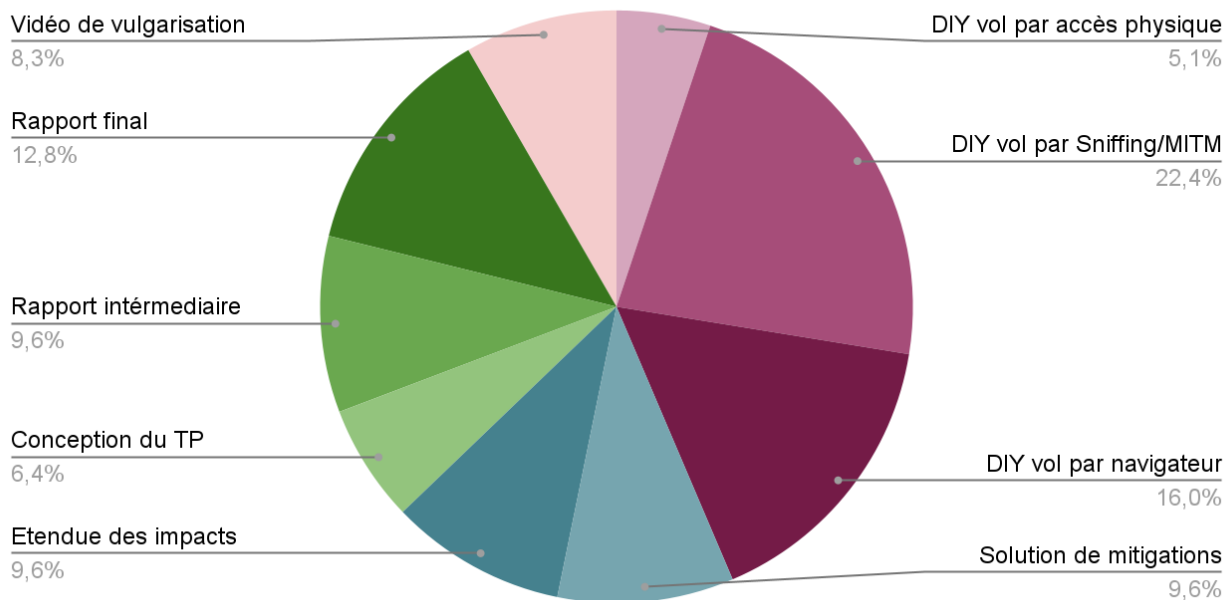


Diagramme de gantt estimé

			Novembre					Décembre				Janvier				Février				Mars				
Titre de la tâche	Date de début	Date fin estimée	31/10	07/11	14/11	21/11	28/11	05/12	12/12	19/12	26/12	02/01	09/01	16/01	23/01	30/01	06/02	13/02	20/02	27/02	06/03	13/03	20/03	27/03
DIY vol par accès physique	31/10/2022	21/11/2022																						
DIY vol par Sniffing / MITM	21/11/2022	02/01/2023																						
DIY vol par navigateur	12/12/2022	23/01/2023																						
Solution de mitigations	02/01/2023	20/02/2023																						
Etendue des impacts	02/01/2023	20/02/2023																						
Conception du TP	14/11/2022	23/01/2023																						
Rapport intermédiaire	31/10/2022	23/01/2023																						
Rapport final	16/01/2023	27/03/2023																						
Vidéo de vulgarisation	20/02/2023	27/03/2023																						
Romane Alternance : semaine en entreprise																								
Roméo : vacances scolaires																								
Romane / Roméo : Semaine de partiels																								