VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
BRNO UNIVERSITY OF TECHNOLOGY

FAKULTA INFORMAČNÍCH TECHNOLOGIÍ
FACULTY OF INFORMATION TECHNOLOGY

ÚSTAV INFORMAČNÍCH SYSTÉMŮ
DEPARTMENT OF INFORMATION SYSTEMS

ODCHYTÁVÁNÍ COOKIES

COOKIES CATCHING

SEMESTRÁLNÍ PROJEKT
TERM PROJECT

AUTOR PRÁCE **DAVID HUDÁK**
AUTHOR

VEDOUCÍ PRÁCE **Mgr. Ing. PAVEL OČENÁŠEK, Ph.D.**
SUPERVISOR

BRNO 2021

Abstrakt

Tato práce se zabývá řešením semestrálního projektu věnovaném trasování cookies v systému Wireshark

Abstract

This thesis deals with past web black market known as Silk Road. This thesis also deals with with theoretical problematics of today's darkweb in context of black markets.

Klíčová slova

cookies, sušenky, wireshark

Keywords

cookies, wiresharl

Citace

HUDÁK, David. *Odchytávání cookies*. Brno, 2021. Semestrální projekt. Vysoké učení technické v Brně, Fakulta informačních technologií. Vedoucí práce Mgr. Ing. Pavel Očenášek, Ph.D.

Odchytávání cookies

Prohlášení

Prohlašuji, že jsem tuto semestrální práci vypracoval samostatně pod vedením pana Pavla Očenáška. Uvedl jsem všechny literární prameny, publikace a další zdroje, ze kterých jsem čerpal.

.....
David Hudák
22. dubna 2021

Poděkování

Rád bych poděkoval panu Očenáškovi za vedení této práce a jeho práce při vedení předmětu IBS.

Obsah

Kapitola 1

Teoretický úvod

S cookies se setkal prakticky každý, kdo někdy použil internet. Jedná se o data uložená na klientském zařízení sloužící k tomu, aby uživatel nabyl jakéhosi domáckého dojmu (proto cookies – sušenky). Tato data uživatel shromažďuje prakticky při každé návštěvě nějaké internetové stránky, přičemž se vytváří při prakticky každé personalizovatelné akci (například kliknutí na reklamu, kliknutí na konkrétní typ zprávy u publicistických serverů, při přihlášení, při nákupu nějakého typu zboží atp.) Ve výsledku pak uživatel dostává na základě toho reklamy a doporučení pouze na produkty, o které by mohl dle statistických dat mít zájem[2].

1.1 Právní pohled

Nejvýraznější regulací cookies v rámci České republiky (obecně v evropském prostoru) je evropská legislativa známá především pod názvem GDPR (Obecné nařízení o ochraně osobních údajů, v originále General Data Protection Regulation). Ta spotřebitelům (klientům webových aplikací) zajišťuje, že uživatel nesmí dostat žádnou cookie, dokud k tomu sám nedá souhlas (výjimka platí pouze pro cookies, která jsou nutná pro základní funkčnost webu). Právní úprava GDPR také rozlišuje dva druhy cookies, a to jsou tzv „First-party cookies“ a „Third-party cookies“. First-party cookies jsou takové, které umísťuje sám web, který uživatel navšťevuje. Third-party cookies zase umísťuje jiná strana než web, který navšťevujeme. Může to být buď provozovatel reklamy, nebo nějaký nástroj pro analýzu dat[1].

1.2 Z hlediska sítí

Cookies jsou součástí HTTP protokolu. V případě, že server chce uložit cookie na klientské zařízení, zašle zařízení zprávu `Set-cookie` s cookie informací. V případě, že se připojuje klientské zařízení na server, součástí žádosti GET o zaslání obsahu stránky je požadavek `Cookie` s následující cookie zprávou[3].

Kapitola 2

Situace

V této kapitole budou popsány nutné prerekvizity pro provedení daného přenosu a samotný experiment.

2.1 Nastavení prohlížeče

Pro tento demonstrační pokus bylo zvoleno prostředí Microsoft Edge. Je tomu tak z toho důvodu, že se nejedná o primární používaný prohlížeč, tudíž by mělo více docházet k výměnám cookies ve směru server→klient. Dále je nutné vypnout veškerá omezení trasování ze strany prohlížeče (Microsoft Edge jej má ve výchozím stavu spuštěný), jelikož by to mohlo ovlivnit výsledky experimentů.

Dalším problémem, který se zpočátku projevoval, bylo obecné zaklikávání jako „Ne“ na všechna nepovinná cookies, což bylo třeba na testovaných serverech zrušit (bylo jich více, než je uvedeno v situacích, avšak pouze na pár z nich se povedlo jasně separovat odeslaná cookies).

2.2 Nastavení Wiresharku

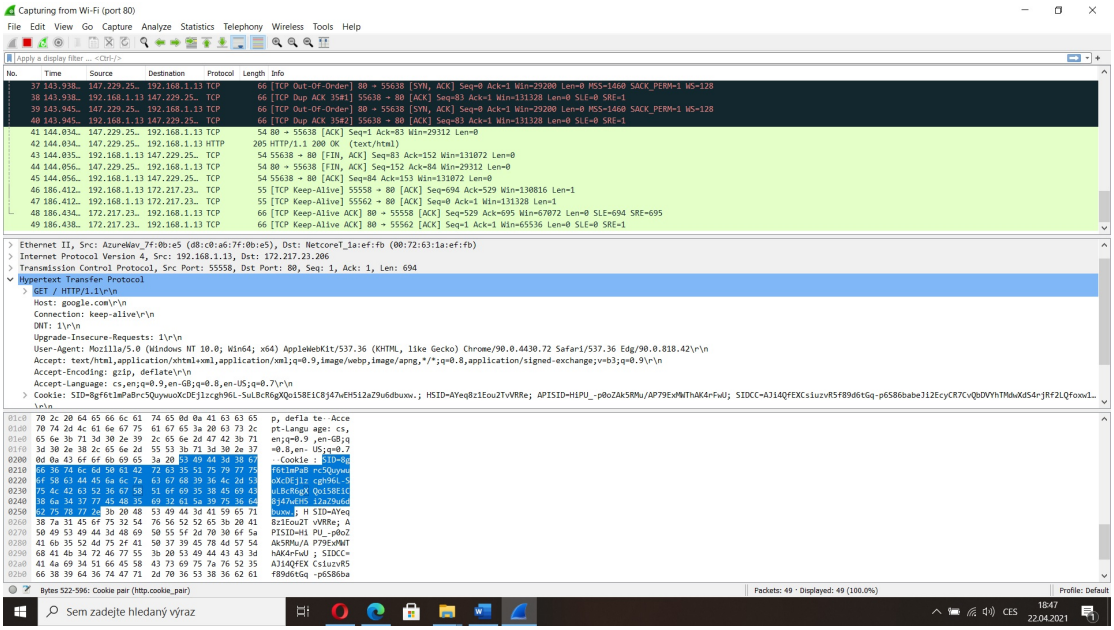
Pro pořízení obou snímků obrazovky bylo použito filtrování pro TCP a UDP spojení s omezením portu na HTTP, v rámci kterého bývají cookies odesílány. Dále bylo zvoleno standarní přípojení přes WiFi, které sice zabírá veškeré připojení, avšak díky filtrování nebyly ostatní pakety příliš rušivé.

2.3 Situace 1 – odchycení paketu s odesílaným cookie

První situace vznikla pouze samotným zavoláním vyhledávače Google, u kterého bylo počítáno s velkým množstvím cookies s ohledem na provozování služby Google Analytics[1]. Paket má přímo v prvním paketu s protokolem HTTP a zprávou `GET` uveden dodatek `Cookie` s následnými SID daných cookies. Celou situaci je pak možné vidět na ilustraci 2.1. Vzhledem k mírnému používání prohlížeče a celkově menšímu množství cookies se dá říci, že experiment proběhl dle očekávaných předpokladů.

Odeslaná cookies mohla být jak druhu first-party (interní Google, vlastním Gmail účet), tak third-party.

[1] Viz https://analytics.google.com/analytics/



Obrázek 2.1: Cookies odesílané serveru Google.com

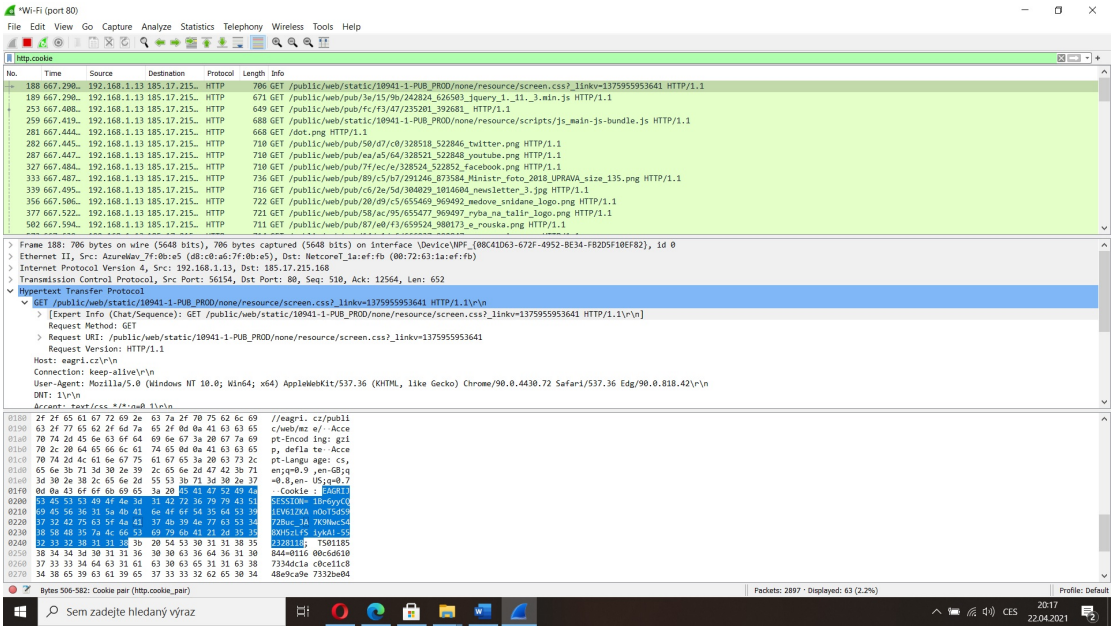
2.4 Situace 2 – odchycení paketu na serveru bez https

Zajímavým odhalením byl fakt, že současné Ministerstvo zemědělství na svém webu[2] nevyužívá moderní protokol se šifrováním https, avšak pouze základní http. To vedlo k situaci, že se dalo využít základní filtrování http.cookie v rámci Wiresharku oproti předchozímu pokusu, kde bylo možné využít pouze filtrování na TCP/UDP protokol a port 80 (http) a následně bylo nutné hledat informaci o cookies ručně. Ilustraci můžeme vidět zde 2.2. Za neočekávané se dá považovat celkově velké množství zpráv odesílajících informaci o cookies. Osobně to vnímám dvěma možnými způsoby – web ministerstva zemědělství je zastaralý, a tak poněkud nešťastně opakuje požadavek o zaslání cookies. Druhá možnost může být, že ministerstvo zemědělství žádá o všechna uložená cookies, jelikož nemá správně nastavené filtrování toho, co žádá.

Celkově k zamyšlení u tohoto experimentu je samotný fakt, že celkově významná instituce používá pouze zastaralý, nezabezpečený a nešifrovaný protokol http místo https. Z hlediska zabezpečení komunikace vůči případným odposlechům se zcela zjevně nejedná o šťastné řešení.

Dalším možným faktem, které je záhodno dodat je, že server Ministerstva zahraničí byl navštíven poprvé, tudíž se muselo jednat o third-party cookies.

[2] Viz http://eagri.cz/public/web/mze/



Obrázek 2.2: Cookies odesílané stránkám Ministerstva zemědělství

2.5 Situace 3 – cookie ze strany serveru

Situaci, kdy by bylo v experimentu přímo vidět, jaká nová cookies přináší http protokol do zařízení, se zachytit nezdařilo. Pravděpodobně to není z toho důvodu, že by k takové situaci nedocházelo, pouze většina moderních serverů používá https protkol, který více šifruje zprávy a informaci o novém cookie šifruje též. Tudíž se experiment nezdařil a taková situace nebyla zachycena.

Kapitola 3

Zhodnocení

Při experimentu se nezdařilo zachytit dostatečně patrnou informaci o přijetí a nastavení nového paketu ze strany serveru. Na druhou stranu se povedlo odhalit zásadní bezpečnostní nedostatek Ministerstva zemědělství.

Z hlediska zachycených paketů se celkově úspěšně dařilo odhalovat odesílaná cookies směrem k serverům. Na základě této informace se pak dále dá pracovat s databází uložených cookies a následně z toho implikovat, jaké údaje od nás která stránka získává.

Naopak se nezdařilo najít informace, které servery do lokálního zařízení ukládají. K vyřešení této situace by teoreticky pomohla práce s šifrovacími klíči a následným dešifrováním zpráv, které přichází (zkrátka to dělat tak, jak to dělají běžně prohlížeče za uživatele).

Literatura

[1] European Parliament. *Cookies, the GDPR, and the ePrivacy Directive*. EU, Naposledy viděno. Dostupné z: https://gdpr.eu/cookies/.

[2] Kaspersky Lab. *What are Cookies?* AO Kaspersky Lab, Naposledy viděno 22. 4. 2021. Dostupné z: https://www.kaspersky.com/resource-center/definitions/cookies.

[3] Velagapudi, S. L. a Gupta, H. Privacy, Security Of Cookies In HTTP Transmission. In: IEEE, ed. *2019 4th International Conference on Information Systems and Computer Networks (ISCON)*. 2019, s. 22–25. DOI: 10.1109/ISCON47742.2019.9036289. ISBN 978-1-7281-3652-3.