Week 5

Week 5a Cookies en fingerprinting

Hoe werkt het web

De browser die je gebruikt (Firefox, google Chrome etc.) stuurt een berichtje naar de webserver van de site die je wilt bezoeken, hierin staat een commando ‘get index.html’ waarop de webpagina terugstuurt <html><titel>(willekeurige site).nl</title>. Ditzelfde gebeurd ook voor elke afbeelding op een pagina (stuk voor stuk wordt opgehaald nadat de pagina is opgehaald!)

Het web is ‘stateless’

Elk verzoek is een verzoek op zich, al deze verzoeken staan los van elkaar en zijn in feite anoniem. De webserver kan niet zien dat één computer meerdere aanvragen doet.

Maar stel dat je 10 artikelen hebt geselecteerd bij bol.com, hoe houdt de webserver dit dan bij elkaar?

Oplossing: cookies!

- Een cookie is een naam/attribuut + waarde, bijvoorbeeld m.b.t. taal. Het attribuut is ‘language’ en de waarde is ‘dutch’.
- Cookies zijn specifiek voor één website. Elke site heeft zijn eigen cookies die worden opgeslagen in de cookiejar. Wanneer je de website opnieuw bezoek of een nieuwe aanvraag doet stuurt je webbrowser de cookies in de jar mee met zijn verzoek.
- Op die manier krijg je dus direct een site bijvoorbeeld in het Nederlands te zien.

In detail

Kom ik voor het eerst op een site dan worden cookies ‘geplaatst’ dat betekent dus dat een ‘nieuwe’ cookie in de jar wordt gezet. Dit ziet er als volgt uit

Set-Cookie: PREF=ID= 123…. Let op, dat er in de rij tekens een verwerkingsdatum is verwerkt

Bezoek ik daarna diezelfde site opnieuw wordt de cookie die bij die site hoort uitgelezen uit de cookie jar en meegestuurd in het verzoek naar de webserver, dit ziet er dan zo uit

Cookie: PREF=ID=123…

Http referer

Iedere keer dat je op een link klinkt waar een verwijzing plaatst vindt wordt de URL van de pagina waar die link staat mee gestuurd. Dat betekent dat de webpagina waar de link naar verwijst weet waar de aanvraag vandaan komt. Dit noem je **third party cookies**

Stel, via google Chrome haal ik een webpagina op bij nu.nl, dan stuurt Chrome een verzoek naar de webserver van nu.nl. dan zit er een **web bug** van 1 pixel groot in de site verwerkt die op de webserver staat van doubleclick by google (die veel wordt gebruikt om websurf gedrag te volgen). Dan gebeurt er onder water

GET afbeelding X

Host: doubleclick.net, De server waar die afbeelding opstaat is dus doubleclick en niet nu.nl,

Referer: http://nu.nl/, je wordt dus bij je bezoek aan nu.nl zonder dat je het doorhebt door verwezen door nu.nl naar doubleclick met je aanvraag voor die ene afbeelding die je helemaal niet kan zien (de web bug).

Cookie: hierin staat een identifier vermeld waarin staat dat je van nu.nl komt.

Wat betekent dit nu,

Stel dat je als niet facebook gebruiker via een link toch facebook bezoekt, dan zou je denken dat facebook niets van je weet omdat je geen account hebt. Dit systeem brengt mee dat je dus via die referer een aanvraag doet en er een ID in de aanvraag wordt meegestuurd en dus in je cookies terecht komt.

Op deze manier kan facebook dus altijd tracken wat welke gebruiker doet met of zonder account!

Tracking met first party cookies

Hiermee accepteer je alleen cookies van de pagina's die je bezoek, al kan dit alsnog leiden tot het tracken wanneer het volgende gebeurt.

Als gebruiker stuur je een verzoek naar een webserver, maar de webpagina is vernieuwd of vervangen. Dan stuurt de webserver waar je in eerste instantie een verzoek naar hebt gestuurd dit verzoek door naar de webserver met de 'juiste' inhoud. Deze stuurt een cookie terug naar de 1e webserver die vervolgens de cookie weer naar de aanvrager stuurt, met een kleine omweg dus hetzelfde resultaat als third party tracking.

Browser fingerprinting

Andere manieren van tracken, dit kan in de vorm van verschillende methoden

- In de aanvraag kan bijvoorbeeld worden verwerkt welk type browser je gebruikt, op deze manier wordt dus getrackt welke software je gebruikt.
- Javascript
  - Scripts hebben toegang tot cookies
- Andere vormen van opslag
  - Flash
  - HTML 5
  - Evercookies

Het tegengaan

- Leegmaken van de cookiejar
- Cookies blokkeren
- Third party cookies niet toestaan
- Plugins tegen cookies scrips en webbugs, bijvoorbeeld 'NoScript'

Week 5b overige digitale sporen

Sporen laat je ook achter na op je eigen pc, netwerkverbindingen, op je telefoon en in de fysieke wereld

Je eigen bestanden, logbestanden

Je eigen computer houdt veel gegevens bij in logbestanden, wat je gedaan hebt op welke tijd. Dit wordt uitgevoerd door je operating system. Denk metadata of bestanden zelf. Maar ook gebruikte applicaties, web en bel geschiedenis bijvoorbeeld.

Dit kan erg relevant zijn in de opsporing van criminele activiteiten.

Netwerkverbindingen

- MAC-adressen (WiFi/Bluetooth tracking)
  Unieke hardware van een netwerk interface dat door ieder acces point opgevraagd kan worden wanneer WiFi of Bluetooth aanstaat.

Voorbeeld: de verkeersinformatie dienst trackt hoeveel auto's er langs een bepaald punt rijden, dit doen ze niet door de auto's te tellen maar door te tellen hoeveel bluetooth signaleren er passeren.
- Eerder bezochte WiFi netwerken
  Je mobiel of laptop zendt je eerder bezochte netwerken uit wanneer WiFi aanstaat
- Data die je verstuurt of ontvangt.
  Denk aan een onveilige verbinding, of wanneer je in hebt gelogd met accounts

Mobiele telefoons

- Gesprekken, tijd, duur en gebelde nummer, locatie
- SMS, tijd, geadresseerde, verstuurde bericht, locatie
- Precieze locatie bepaling, door driehoeksmeting of trilateration

Op het internet

- IP-pakketten, data + IP-adres (betekent, afzender + bestemming)
- IP-adres is te herleiden tot een fysieke locatie, geolocation
- IP-poort geeft aan welk type dienst

Smartphone

- Op je smartphone zitten allerlei censoren die van alles en nog wat meten, denk aan gyroscoop en GPS die informatie genereren.

Gebruik van diensten

- Wanneer je een website bezoekt word je bijgeschreven in de acces logs
- Sociale netwerken, denk aan het worden getagt in een afbeelding
- Het web, zelfs je muisbewegingen worden getrackt
- Mailbox, wat verzonden en wat ontvangen

De fysieke wereld

Je fysieke locatie wordt ook getrackt wanneer je in de fysieke wereld loopt, denk aan met je bluetooth door een stad lopen. Hier kan precies worden gevolgd waar je als zender hebt gelopen d.m.v. MAC-adressen. Maar denk ook aan nummerplaat herkenning en cameratoezicht.

Uit de gegevens kan je directe dingen afleiden zoals locatie en transacties. Indirect kan het meebrengen dat degene die inzicht heeft in je gegevens je politieke voorkeur of zelfs geaardheid kan herkennen.