

Time Is Running Out

Assessing Temporal Privacy of Privacy Zones in Fitness Tracking Social Networks

Wout DELEU

Promotor: Prof. dr. ing. Stijn Volckaert

Begeleiders: Ing. Karel Dhondt,
Ing. Alicia Andries

Masterproef ingediend tot het behalen van
de graad van master of Science in de
industriële wetenschappen: Elektronica/ICT
Optie Smart Applications

Academiejaar 2022 - 2023

©Copyright KU Leuven

Deze masterproef is een examendocument dat niet werd gecorrigeerd voor eventuele vastgestelde fouten.

Zonder voorafgaande schriftelijke toestemming van zowel de promotor(en) als de auteur(s) is overnemen, kopiëren, gebruiken of realiseren van deze uitgave of gedeelten ervan verboden. Voor aanvragen i.v.m. het overnemen en/of gebruik en/of realisatie van gedeelten uit deze publicatie, kan u zich richten tot KU Leuven Technologicampus Gent, Gebroeders De Smetstraat 1, B-9000 Gent, +32 92 65 86 10 of via e-mail iiw.gent@kuleuven.be.

Voorafgaande schriftelijke toestemming van de promotor(en) is eveneens vereist voor het aanwenden van de in deze masterproef beschreven (originele) methoden, producten, schakelingen en programma's voor industrieel of commercieel nut en voor de inzending van deze publicatie ter deelname aan wetenschappelijke prijzen of wedstrijden.

Voorwoord

Het voorwoord vul je persoonlijk in met een appreciatie of dankbetuiging aan de mensen die je hebben bijgestaan tijdens het verwezenlijken van je masterproef en je hebben gesteund tijdens je studie.

Samenvatting

0.1 Situering

In een maatschappij waar sociale media allom aanwezig is, zijn de privacybezorgdheden hier rond evenzeer erg actueel. Bij het ontwikkelen van applicaties moeten privacywetgevingen en -bezorgdheden in acht genomen worden. Maar dit neemt niet weg dat in heel wat applicaties nog gaten te vinden zijn in het privacybeleid. Gedurende deze thesis worden gekende fitness-trackers onder de loep genomen, waaronder Strava. Er is op te merken dat heel wat van deze platformen op gelijkaardige manieren proberen privacy te garanderen. In de meeste gevallen gaat dit over het verbergen van een stuk van de activiteit, en zo de startpositie niet weer te geven op de kaart. Het verbergen van deze activiteit gebeurt door het opstellen van een *Endpoint Privacy Zone*. Hierbij wordt een cirkel opgesteld waarbinnen de afgelegde weg zal worden verborgen. In de paper van K. Dhondt is een manier terug te vinden om door het combineren van verschillende gegeven afstanden (bijvoorbeeld totale afstand, afstand tussen 2 punten, ...) en het bepalen van deze EPZ, de effectieve startpositie van de activiteit te achterhalen en zo dus gevoelige informatie bloot te leggen.

0.2 Doelen

In deze thesis zal geprobeerd worden om alternatieve manieren te vinden om deze gevoelige locatie te bepalen aan de hand van andere metadata zoals snelheid. Hierbij zal ook de effectiviteit ervan geanalyseerd worden, en zal getracht worden om enkele manieren te vinden om de privacy van het platform te verhogen. Er zal getracht worden deze werkwijze toe te passen aan de hand van verscheidene beschikbare metadata.

Abstract

Het extended abstract of de wetenschappelijke samenvatting wordt in het Engels geschreven en bevat **500 tot 1.500 woorden**. Dit abstract moet **niet** in KU Loket opgeladen worden (vanwege de beperkte beschikbare ruimte daar).

Keywords: Voeg een vijftal keywords in (bv: Latex-template, thesis, ...)

Inhoudsopgave

Voorwoord	iii
0.1 Situering	iv
0.2 Doelen	iv
Samenvatting	iv
Abstract	v
Inhoud	vii
Figurenlijst	viii
Tabellenlijst	ix
Lijst met afkortingen	x
1 Inleiding	1
1.1 Situering	1
1.2 Doelstelling	2
2 Achtergrond	3
2.1	3
3 Figuren en tabellen	4
3.1 Algemene richtlijnen	4
4 Richtlijnen voor formules	6
5 Richtlijnen voor referenties	7
5.1 Inleiding	7
5.2 Referentiestijl	7

A Uitleg over de appendices**10**

Lijst van figuren

1.1	Voorbeeldactiviteit Strava	2
3.1	Dit is een voorbeeld van een figuur-float	5

Lijst van tabellen

3.1	Dit is een voorbeeld van een tabel	5
-----	--	---

Lijst van afkortingen

EPZ Endpoint Privacy Zone

Hoofdstuk 1

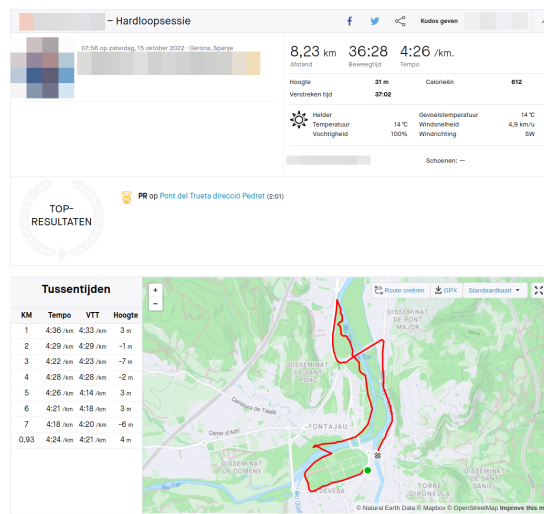
Inleiding

1.1 Situering

Sociale media is zo goed als niet meer weg te denken uit het huidige moderne leven. Sociale media hebben over de jaren verschillende definities gekregen, Philip and Parks definieren sociale media als de infrastructuur en tools om content te maken en te verspreiden[6]. Deze definitie is erg ruim, en vertakt zich dus in heel wat facetten, waaronder sociale netwerken, media sharing networks, . . . En ook de fitnesstrackers. Deze opkomst van nieuwe media brengen echter ook vaak onbedoelde maar significante privacy bezorgdheden met zich mee.

De focus in deze dissertatie ligt op fitnesstrackers, meer specifiek platformen die gps-locaties gebruiken, zoals Strava, Nike Run Club, etc. Dit zijn platformen waar sportactiviteiten zoals lopen, fietsen, wandelen, . . . kunnen worden gedeeld met andere personen. Het algemene concept is hierbij dat wanneer je een sportactiviteit uitvoert, je deze voor je volgers beschikbaar maakt. De sportactiviteit zal dan natuurlijk ook bepaalde gegevens bevatten die zichtbaar zijn, zoals tijdstippen, hartslag, beweegtijd, en vaak ook gps-locaties. 1.1. Vele van deze gegevens hebben direct of indirect een negatieve impact op de privacy van de user. Deze negatieve gevolgen komen dan vooral in de vorm van het onbedoeld vrijgeven gevoelige locaties. Dit kan gaan over woonplaatsen, wat kan leiden tot o.a. stalking. Alsook locaties waar sportmateriaal wordt opgeborgen. Er zijn gevallen bekend van fietsdieven die Strava gebruiken om fietsen te kunnen lokaliseren[7][2]. Grootschaligere voorbeelden die toch het vermelden waard zijn de gevallen waarbij geheime militaire basissen ontdekt worden door het bestuderen van heatmaps.

Deze platformen implementeren elk op zich manieren om de privacy van de users te verbeteren. Hiervoor zijn verschillende manieren mogelijk. De simpelste is misschien wel de mogelijkheid om activiteiten te verbergen voor anderen. Zo kunnen enkel de mensen die de gebruiker expliciet toelaat activiteiten bekijken. Een complexere aanpak is het gebruik van *endpoint privacy zones* (EPZ). Hierbij wordt de weergegeven route voor de persoon die meekijkt gedeeltelijk verborgen. Er wordt als het ware een deel van de route afgekap, en het eind- en startpunt worden verschoven. Het be-



Figuur 1.1: Voorbeeldactiviteit Strava

gin -en eind-deel van de route wordt dus onzichtbaar enkel voor de andere gebruikers. Het valt op dat deze profielen erg bewust zijn van de mogelijke gevaren van hun platformen. Echter is er een afweging te maken bij de implementatie tussen de bruikbaarheid van het platform, en de privacy van de eindgebruiker. Hoe meer info wordt vrijgegeven, hoe groter de kans om mogelijk schade-lijke private info wordt meegegeven. Aan de andere kant, bij het weglaten van informatie gaat de gebruiksvriendelijkheid en de aanwezigheid van nuttige info van het platform serieus achteruit gaat.

1.2 Doelstelling

Het doel van deze scriptie is om private locaties (verborgen start- en eindlocaties) van een acti-viteiten te achterhalen, ondanks het gebruik van de EPZ als privacy beveiligingsmechanisme. In het verleden werden enkele manieren beschreven om a.d.h.v. andere metadata zoals hoogtedata en afstanden de EPZ te omzeilen (*Dhondt et al., Verdonck*). Hier wordt meer in detail gegaan op het gebruik van snelheidsdata. Als basis voor deze aanval wordt de inferentie aanval op de EPZ van Dhondt et al. genomen. Er wordt dan onderzocht of deze aanval nog succesvol kan worden uitgevoerd bij het weglaten van gegevens, en dus door het gebruik van andere gegevens, voorna-melijk snelheid.

Om deze doelstelling te bekomen zal eerst een analyse op de afwijkingen van tussen de bere-kende afstanden nodig om de inferentie aanval uit te voeren, en de waarden afgeleid volgens de berekeningen van Dhondt et al.. Dit zal gebeuren

Hoofdstuk 2

Achtergrond

2.1

Hoofdstuk 3

Figuren en tabellen

3.1 Algemene richtlijnen

Alle figuren en tabellen worden genummerd en binnen een float omgeving geplaatst

```
(\begin{figure} figuurcontent \end{figure})
```

Foto's, grafieken, schema's,... worden alle onder de benaming 'Figuur' gecatalogeerd.

Het is belangrijk dat tabellen en figuren duidelijk zijn en dat ze alle informatie bevatten die nodig is om ze te begrijpen.

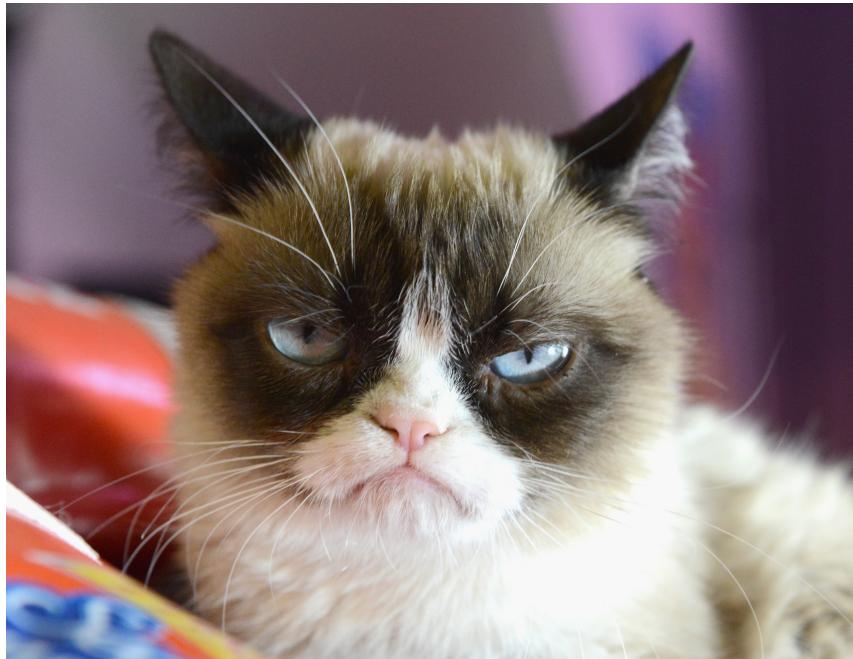
Tabellen worden bij voorkeur niet gesplitst over twee bladzijden. Indien een tabel niet op één bladzijde past, wordt het bijschrift op de volgende bladzijde hernomen en aangevuld met (vervolg). Ook de kolomkoppen van de tabel worden hernomen.

In de tekst wordt naar alle tabellen en figuren verwezen met het itemnummer. Schrijf dus niet 'onderstaande figuur toont....', maar wel 'Figuur 3.1 toont...'. Doe dit door gebruik te maken van de commando's `\label{}` en `\ref{}`. Geef figuren ook zinvolle captions (`\caption{Caption}`). Figuren worden gecentreerd op de bladzijde. Ook het bijschrift wordt gecentreerd en onder de figuur geplaatst. Na de figuurnummer volgt een de beschrijving van de figuur.

Figuur 3.1 toont een voorbeeld gegeven van een float omgeving voor een figuur. Hieronder wordt de syntax weergegeven.

```
\begin{figure}[!ht]
\centering
\includegraphics[width=0.75\linewidth]{image.jpg}
\caption{Dit is een voorbeeld van een figuur-float}
\label{fig:VoorbeeldFigFloat}
\end{figure}
```

Tabellen worden links uitgelijnd op de bladzijde. Ook het bijschrift wordt links uitgelijnd en boven de tabel geplaatst. Na de tabelnummer volgt de beschrijving van de tabel. Tabel 3.1 toont een voorbeeld van een eigen tabel. Vermijd om tabellen te kopiëren van andere werken, maar herwerk ze en plaats de nodige bronvermelding. De nodige syntax om tabel 3.1 te generen wordt hieronder



Figuur 3.1: Dit is een voorbeeld van een figuur-float

weergegeven:

```
\begin{table}[!ht]
\caption{Dit is een voorbeeld van een tabel}
\begin{tabular}{ccc}
\hline
Kolom 1 & Kolom 2 & Kolom 3\
\hline
1 & 2 & 3\\
4 & 5 & 6\\
\hline
\end{tabular}
\label{tab:VoorbeeldTableFloat}
\end{table}
```

Tot slot, let er op dat er expliciet naar elke tabel en figuur verwezen wordt vanuit de tekst.

Tabel 3.1 Dit is een voorbeeld van een tabel

Kolom 1	Kolom 2	Kolom 3
1	2	3
4	5	6

Hoofdstuk 4

Richtlijnen voor formules

Er zijn twee manieren om formules in LaTeX in te voeren:

- Inline: $a^2 + b^2 = c^2$ (`$a^2+b^2 = c^2$`)
- In een equation omgeving (`\begin{equation} a^2+b^2 = c^2 \end{equation}`):

$$a^2 + b^2 = c^2 \tag{4.1}$$

Griekse letters geef je in d.m.b. het backslash commando. Bijvoorbeeld de letter sigma σ verkrijg je door `σ` inline in te geven. Dit is analoog voor griekse letters in de equation omgeving. Een beknopte lijst van symbolen vind je op de Wikibooks pagina voor LaTeX ([link](#)). Alle andere nuttige informatie omtrent het gebruik van LaTeX voor formules vind je hier ook terug.

Hoofdstuk 5

Richtlijnen voor referenties

5.1 Inleiding

De referentielijst bevat de volledige lijst van literatuur en bronnen waarnaar in de tekst wordt verwezen. Door systematisch de referentielijst aan te vullen bij het schrijven van het literatuuroverzicht gaat er achteraf geen tijd verloren aan het opnieuw opzoeken van referenties.

5.2 Referentiestijl

Voor het verwijzen naar informatiebronnen wordt gebruik gemaakt van het numerisch systeem of van het auteur-jaar systeem. Dit kies je door volgend commando in het latex bronbestand aan te passen:

- numerisch (IEEE) : `\bibliographystyle{ieee}`
- alfabetisch (APA) : `\bibliographystyle{apalike}`

Plaats je bronnen in een *bibtex* bestand (evt. via software zoals bv. Jabref Endnote of Mendeley), waarnaar je verwijst vanuit je thesis text a.d.h.v. het commando `\cite`. Enkele links naar nuttige software in deze context:

- JabRef (Open Source)
- Mendeley (Freeware)
- EndNote (Paid license)

Indien je zelf een *.bibtex* bestand wil aanleggen dien je volgende syntax te volgen voor een tijdschriftartikel:

```
@article{hughes2005,  
title={Isogeometric analysis: CAD, finite elements, NURBS, exact geometry  
and mesh refinement},  
author={Hughes, Thomas JR and Cottrell, John A and Bazilevs, Yuri},  
journal={Computer methods in applied mechanics and engineering},  
volume={194},  
number={39},  
pages={4135--4195},  
year={2005},  
publisher={Elsevier}  
}
```

Enkele voorbeelden van het gebruik van bronnen in een tekst (in APA stijl):

Recent werd het Higgs boson experimenteel vastgesteld door Aad et al. [?] (syntax: \cite{aad2012}).

Als alternatief voor het discretiseren van een CAD model vooraleer een eindige elementenanalyse te kunnen toepassen, stellen Hughes et al. voor om de nodige elementenformulering rechtstreeks uit de NURBS beschrijving van de CAD geometrie te halen [?] (syntax: \cite{hughes2005}). Daarnaast introduceren ze tevens een k-iteratieve procedure als een verfijning van de geldende p- en h-iteratieve procedures in eindige elementen methoden [?] (syntax: \cite{cottrell2009}).

Bibliografie

- [Str] Strava-privacybeleid. <https://www.strava.com/legal/privacy>. (Accessed on 02/20/2023).
- [2] Bowden, A. (2018). Cyclist who had five bikes stolen says thieves are looking for quick times on strava to try and find high-end bikes – warns other users to check their privacy settings — road.cc. <https://road.cc/content/news/248798-cyclist-who-had-five-bikes-stolen-says-thieves-are-looking-quick-times-strava>. (Accessed on 02/20/2023).
- [3] Carr, C. T. and Hayes, R. A. (2015). Social media: Defining, developing, and divining. *Atlantic Journal of Communication*, 23(1):46–65.
- [4] Dhondt, K., Pochat, V. L., Voulimeneas, A., Joosen, W., and Volckaert, S. (2022). A run a day won't keep the hacker away: Inference attacks on endpoint privacy zones in fitness tracking social networks.
- [5] Hern, A. (2018). Fitness tracking app strava gives away location of secret us army bases — gps — the guardian. <https://www.theguardian.com/world/2018/jan/28/fitness-tracking-app-gives-away-location-of-secret-us-army-bases>. (Accessed on 02/20/2023).
- [6] Howard, P. and Parks, M. (2012). Social media and political change: Capacity, constraint, and consequence. *Journal of Communication*, 62.
- [7] Vanmeldert, D. (2022). Sportapp strava laat fietsdieven of stalkers nog altijd meekijken — vrt nws: nieuws. <https://www.vrt.be/vrtnws/nl/2022/10/28/strava-kul/>. (Accessed on 02/20/2023).
- [8] Verdonck, T. (2022). Inferentie-aanvallen met hoogteprofielen tegen (endpoint) privacy zones in fitness tracking sociale netwerken. Master's thesis, KU Leuven. Faculteit Industriële Ingenieurswetenschappen, Leuven. Book Title: Inferentie-aanvallen met hoogteprofielen tegen (endpoint) privacy zones in fitness tracking sociale netwerken.

Bijlage A

Uitleg over de appendices

Bijlagen worden bij voorkeur enkel elektronisch ter beschikking gesteld. Indien essentieel kunnen in overleg met de promotor bijlagen in de scriptie opgenomen worden of als apart boekdeel voorzien worden.

Er wordt wel steeds een lijst met vermelding van alle bijlagen opgenomen in de scriptie. Bijlagen worden genummerd met een drukletter A, B, C,...

Voorbeelden van bijlagen:

Bijlage A: Detailtekeningen van de proefopstelling

Bijlage B: Meetgegevens (op USB)

