Warding off Macavity through threat modeling

Building a personal threat model to shore up against stalkers told through Cats the Musical.

Content Warning

This talk contains mentions of:

- Stalking
- Abusive relationships
- Blatant spoilers for Cats the Musical

The naming of Cats is a difficult matter

- Daniëlle or Dani&euml;lle or Dani�lle or Dany
- DevSecOps consultant
- Member of WICCA,
  - on the org team for WICCON
- Musical lover
  - *Top 0,5% of Andrew Lloyd Webber listeners on Spotify*
- Pancakes look like this here

women 01010111 in 01001001 cybersecurity 01000011 community 01000010 association 01000001

womenofwicca.nl

Why this talk

- It’s not Just Stalkerware - MifareLady, May Contain Hackers 2022

  “Are there any Checklists?”

- Threat Modeling:

  Threat modeling is analyzing representations of a system to highlight concerns about security and privacy characteristics

  threatmodelingmanifesto.org

Threat Modeling

The ~~four~~ *five* questions of threat modeling:

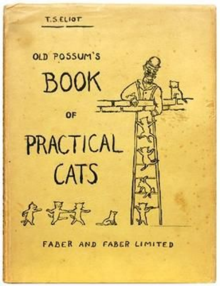
- What are we working on?
- What could go wrong?
- What are we going to do about that?
- Did we do a good enough job?

- And how all this applies to Jellicle Cats?

What’s a Jellicle Cat?

“Hal, it’s about cats.”

- Book: TS Elliot’s *Old Possum’s Book of Practical Cats.*
- Creatives: Andrew Lloyd Webber, Gillian Lynne, Trevor Nunn
- Running productions since 1981
    - Currently: Japan and Oasis of the Seas
- Theatre proshot filmed in 1998
    - (and a CGI movie in 2019)
- Brought innovation to musical theatre



T.S. ELIOT

OLD POSSUM'S

BOOK

OF

PRACTICAL

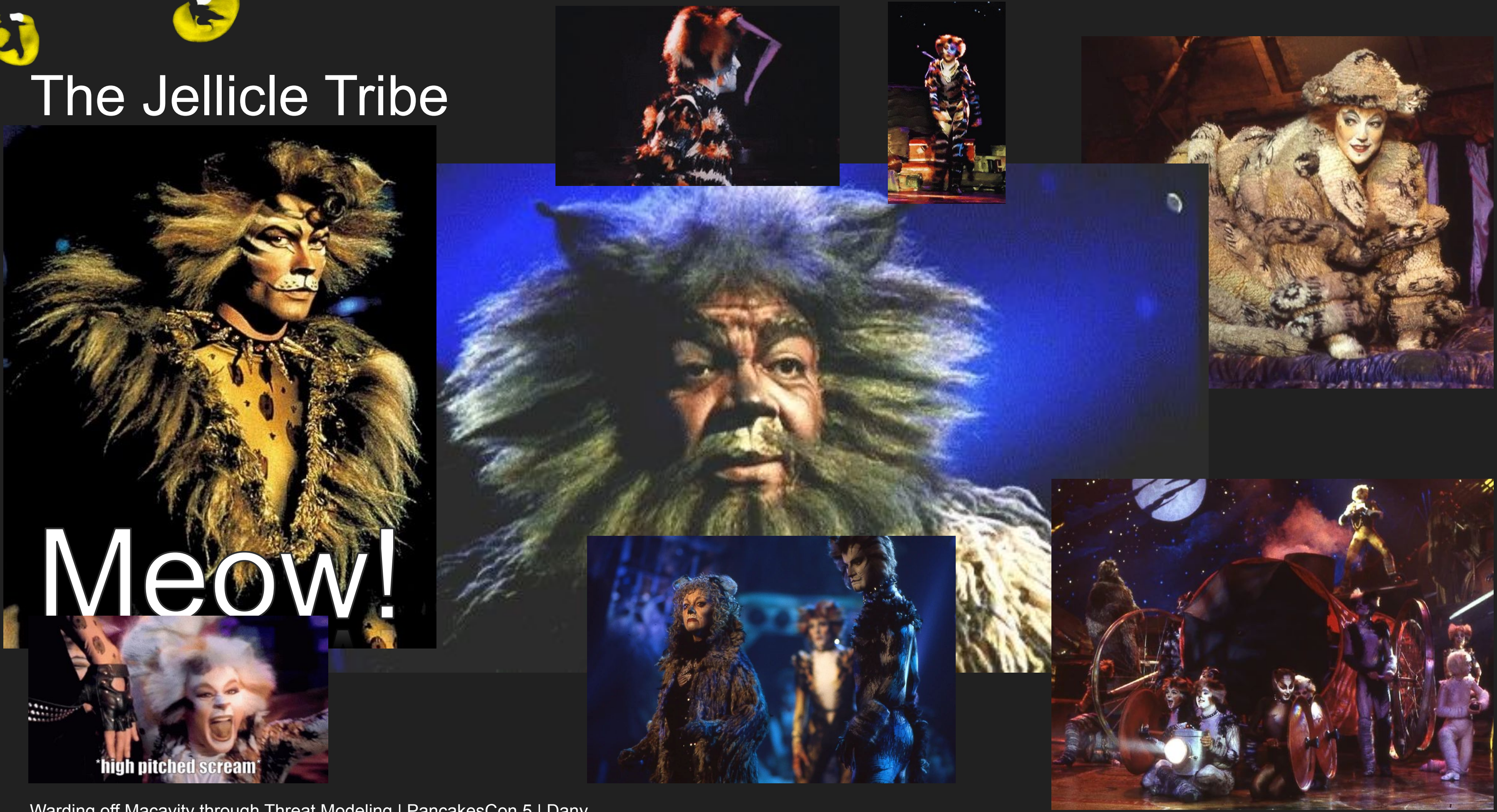
CATS

FABER AND FABER LIMITED

Jellicle Cats meet once a year

Ronacher Theater, Vienna

The Jellicle Tribe



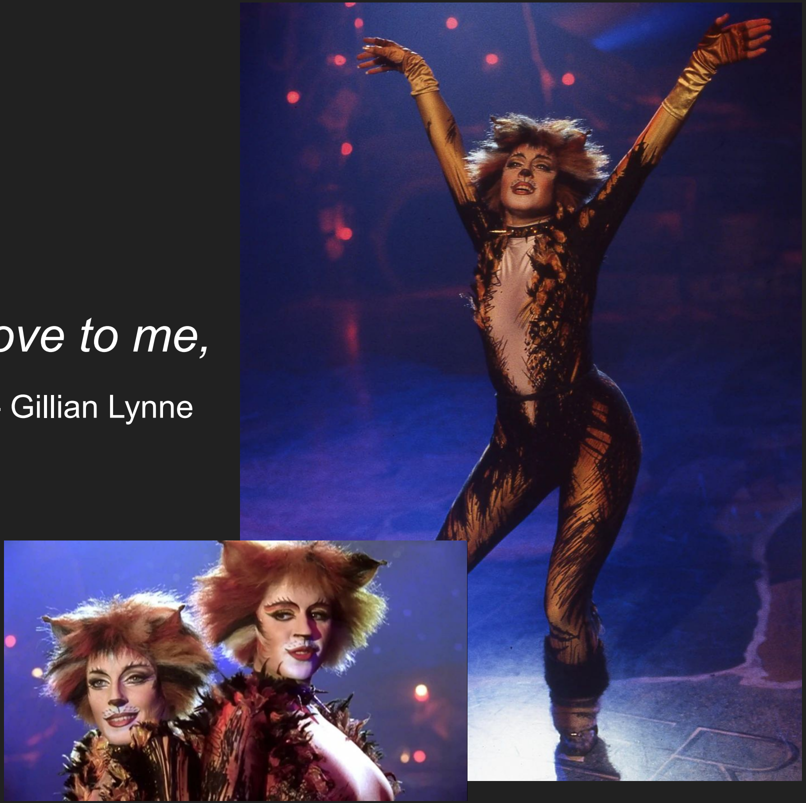
Meow!

Demeter

- *Skittish, Cautious, Paranoid*
- Some connection with Grizabella
- Very good friends with Bombalurina
- Used to date Macavity:

The man was wonderful when he made love to me, but I hated him!”

- Gillian Lynne



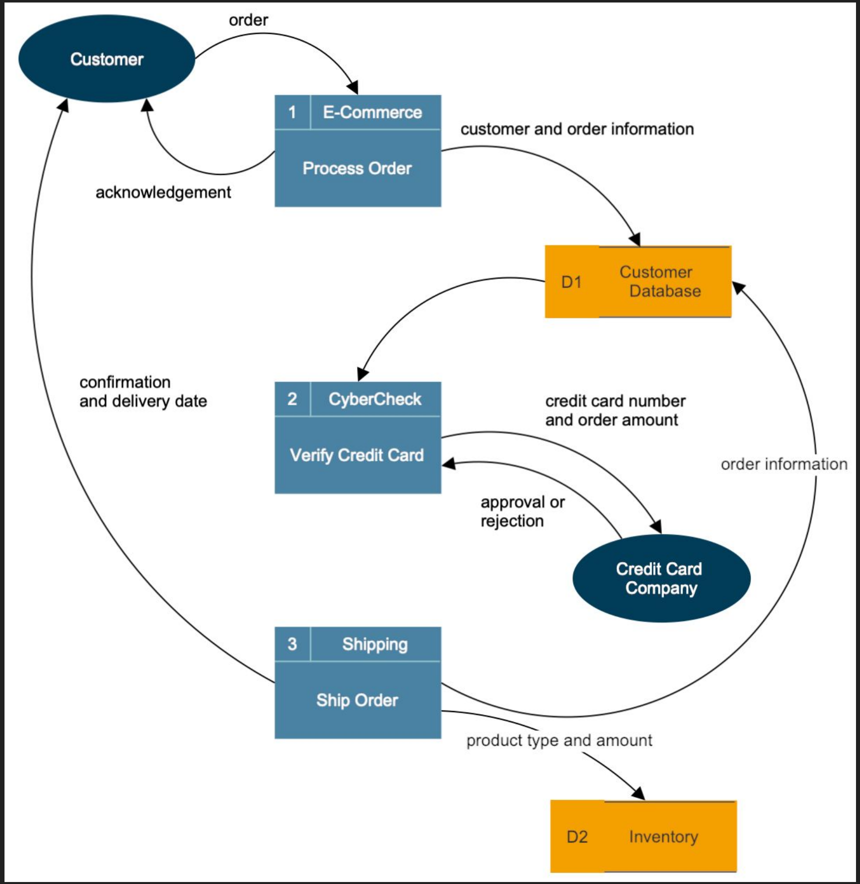
Macavity

- Breaks every human law,
  Breaks the law of gravity
- *Hypnotic, Jealous, Dangerous*
- Inspired by Professor Moriarty
- Namesake of the Macavity Awards for Mystery Fiction
- Would be a great Hacker as he leaves no trace in logs

What are we working on?

A threat model starts with a diagram

Most common is the Data Flow Diagram



What are we working on, a personal DFD

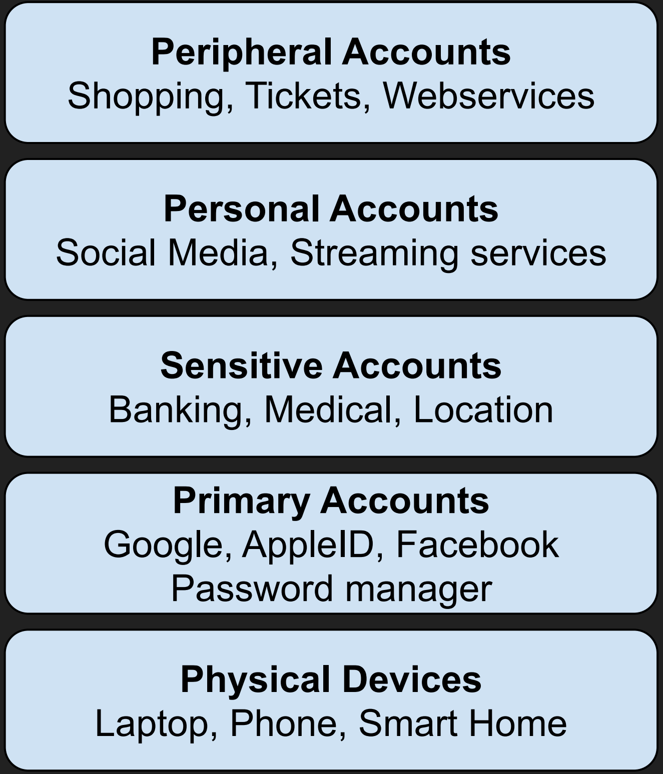
What are we working on?

Divided into categories

Inspired by OSI stack

From most to least sensitive

Assets and accounts can be interlinked



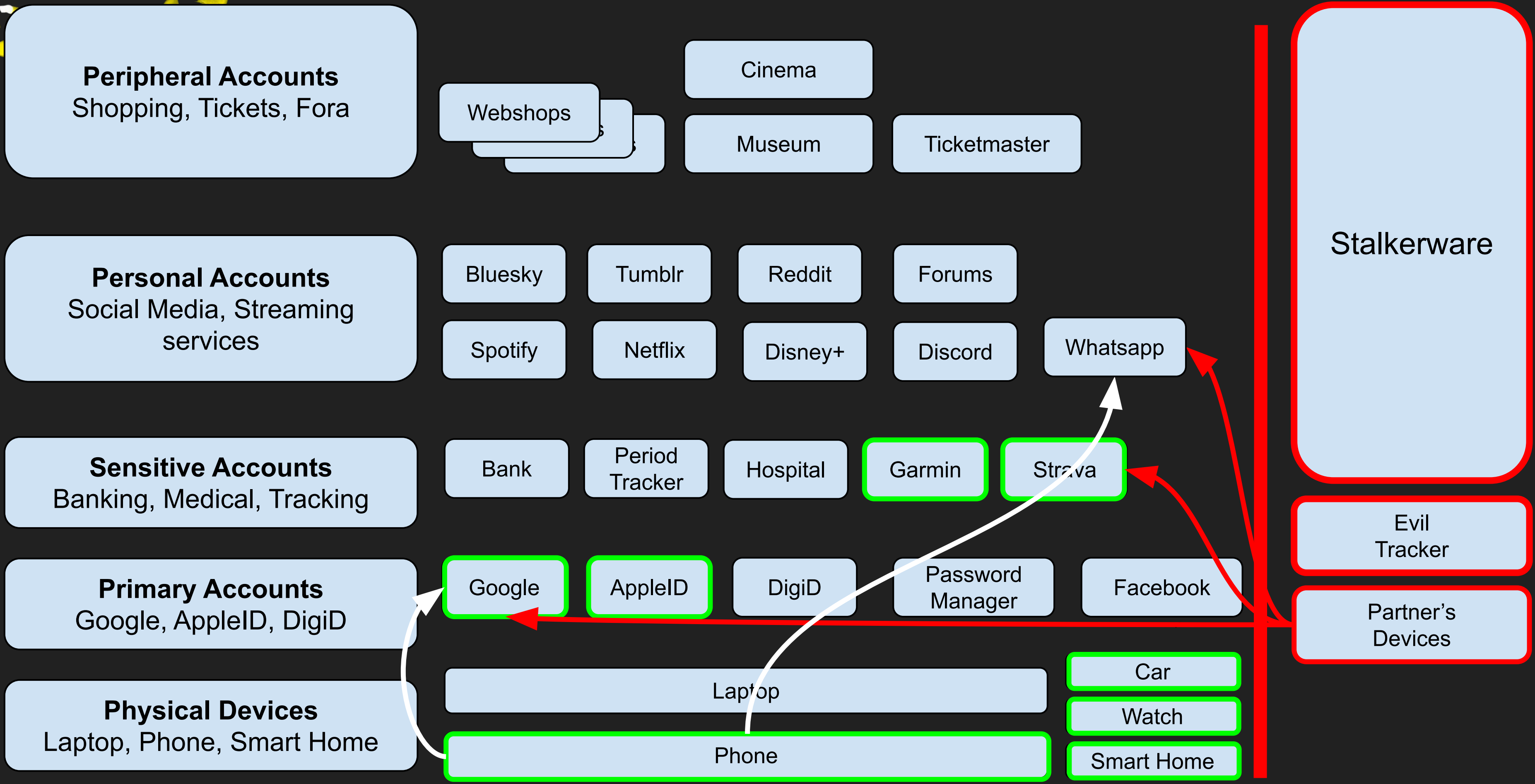
Peripheral Accounts
Shopping, Tickets, Webservices

Personal Accounts
Social Media, Streaming services

Sensitive Accounts
Banking, Medical, Location

Primary Accounts
Google, AppleID, Facebook
Password manager

Physical Devices
Laptop, Phone, Smart Home



Peripheral Accounts
Shopping, Tickets, Fora

Webshops

Cinema

Museum

Ticketmaster

Personal Accounts
Social Media, Streaming services

Bluesky

Tumblr

Reddit

Forums

Spotify

Netflix

Disney+

Discord

Whatsapp

Sensitive Accounts
Banking, Medical, Tracking

Bank

Period Tracker

Hospital

Garmin

Strava

Primary Accounts
Google, AppleID, DigiD

Google

AppleID

DigiD

Password Manager

Facebook

Physical Devices
Laptop, Phone, Smart Home

Laptop

Phone

Car

Watch

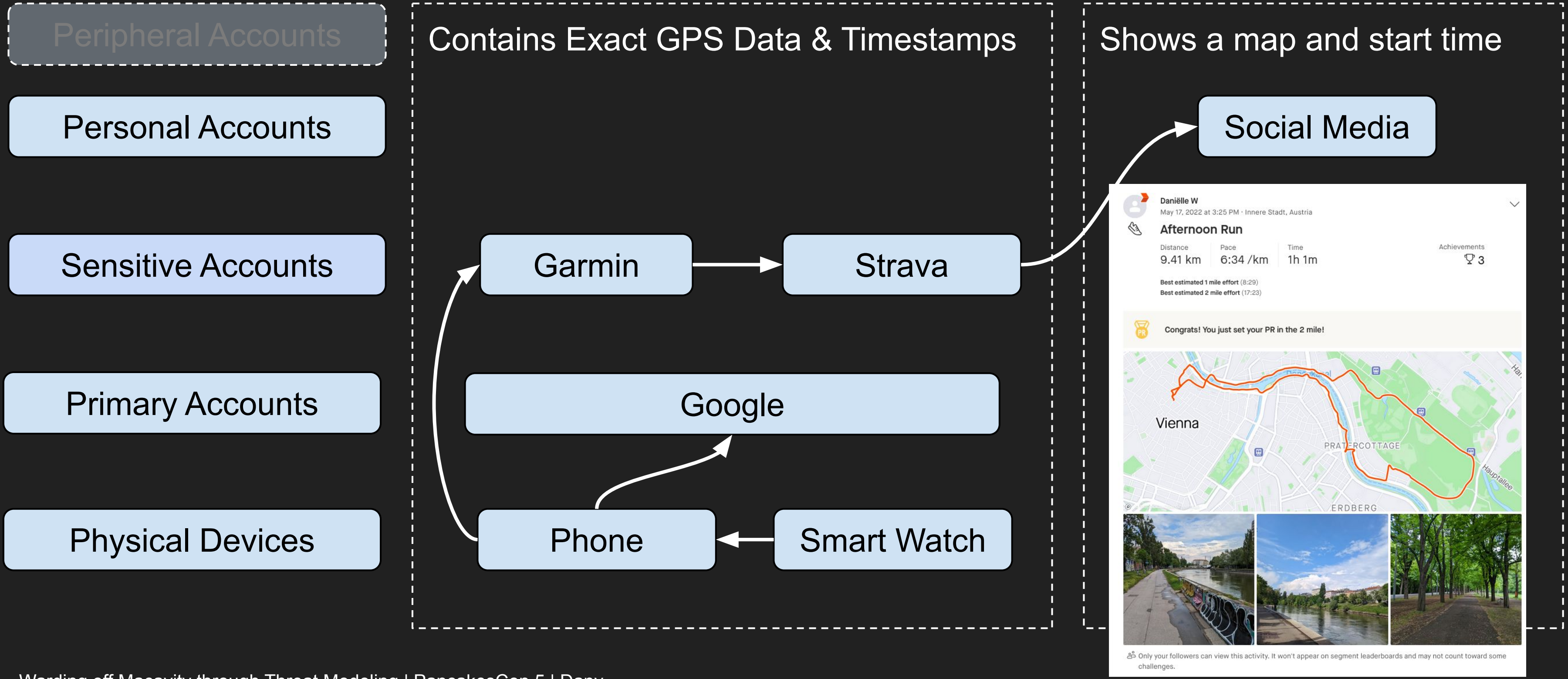
Smart Home

Stalkerware

Evil Tracker

Partner's Devices

Let’s go for a run



Daniëlle W

May 17, 2022 at 3:25 PM · Innere Stadt, Austria

Afternoon Run

Distance	Pace	Time	Achievements
9.41 km	6:34 /km	1h 1m	3

Best estimated 1 mile effort (8:29)
Best estimated 2 mile effort (17:23)

Congrats! You just set your PR in the 2 mile!

Only your followers can view this activity. It won't appear on segment leaderboards and may not count toward some challenges.

Persona non Grata

Who are they?

What is their motivation?

What are their objectives?

How much effort are they willing to put in?

- Perseverance, how much time do they have?
- Skills, what technology are they able to use?
- Funding, how much money are they willing to spend?

Persona: Macavity, the Napoleon of crime

Who: Ex-partner, had access to Demeter’s devices, shared accounts

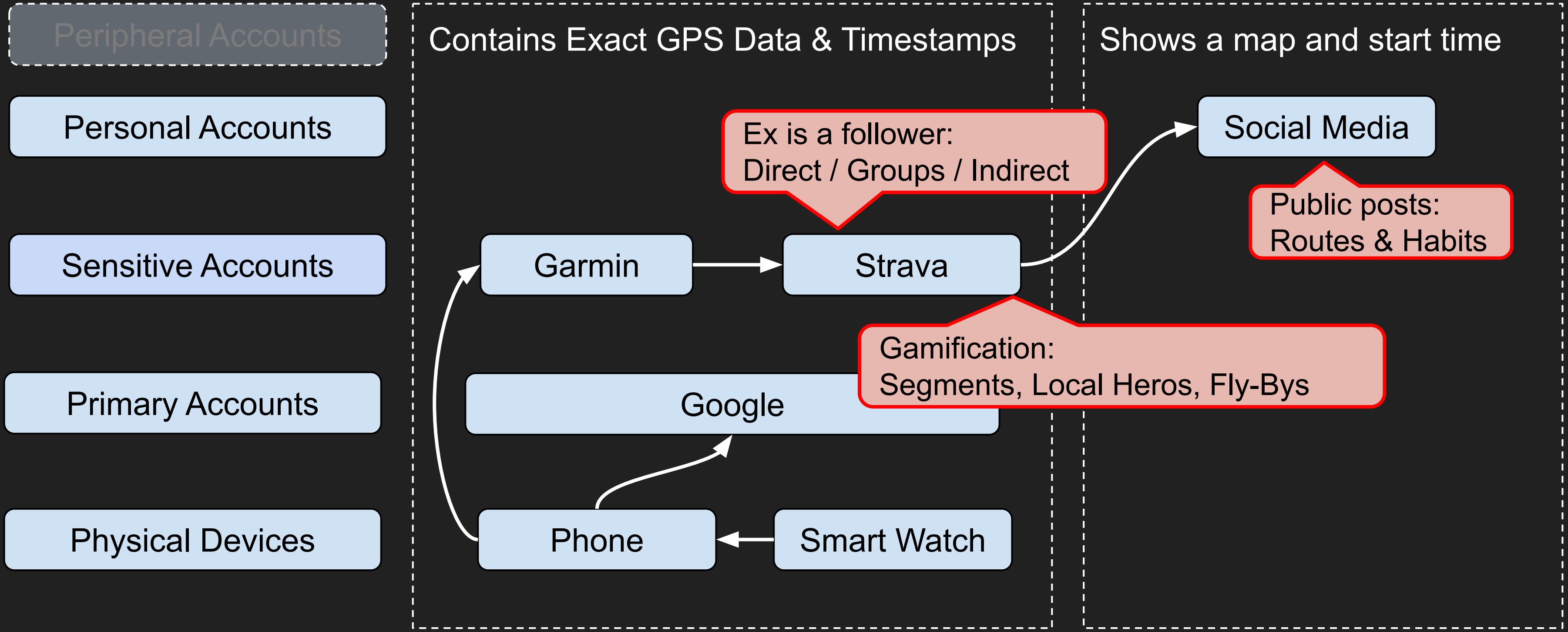
Motivation: Jealousy, feels that she belongs to him, assert dominance

Objective: Track her, exert control, gain physicall access to the ball and take control of the Jellicle tribe.

Effort: Obsessive (plenty of time & perseverance) also has accomplices

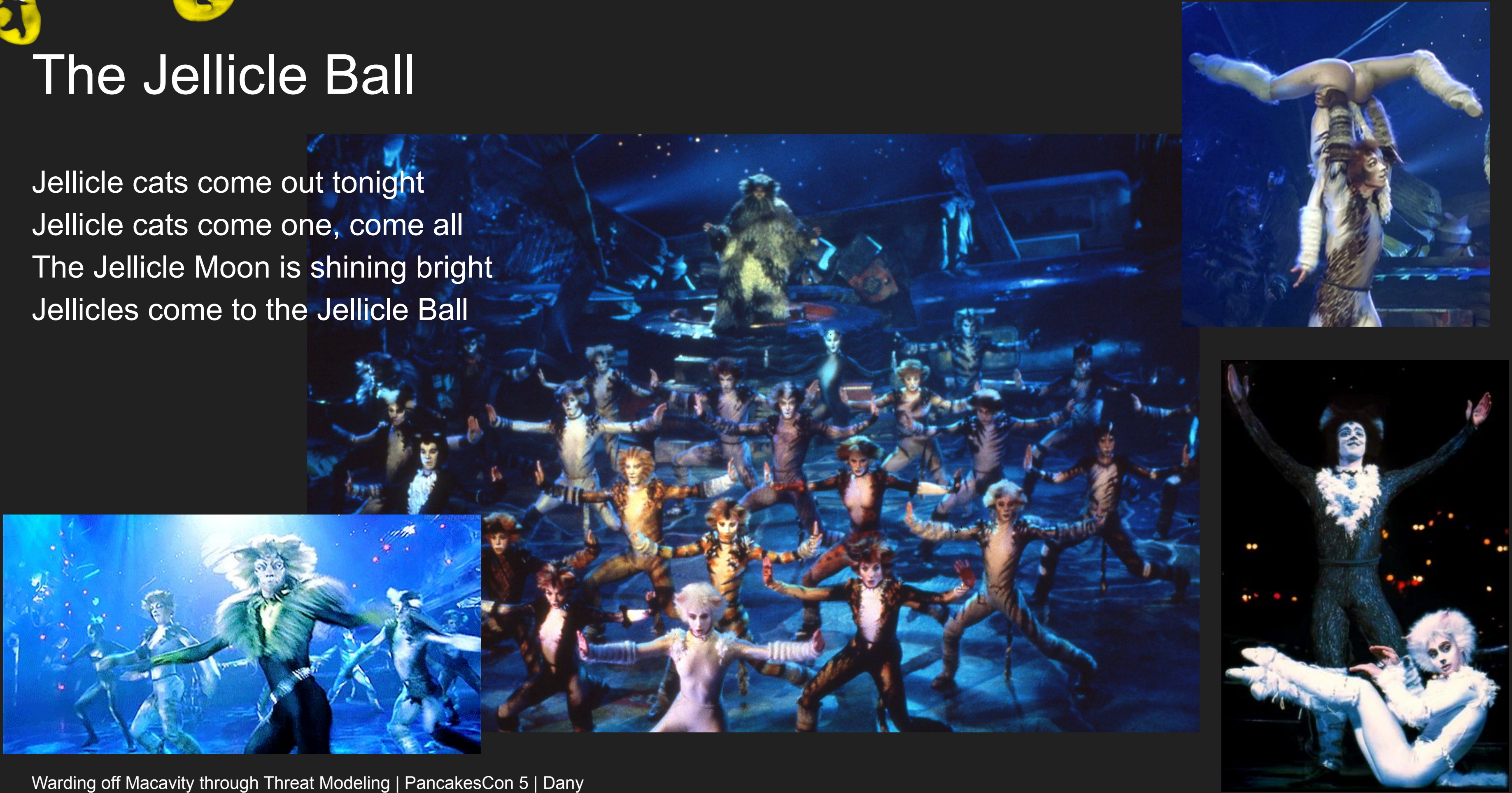
I could mention Mungojerrie,
I could mention Griddlebone.

Threat: Physical stalking during workouts



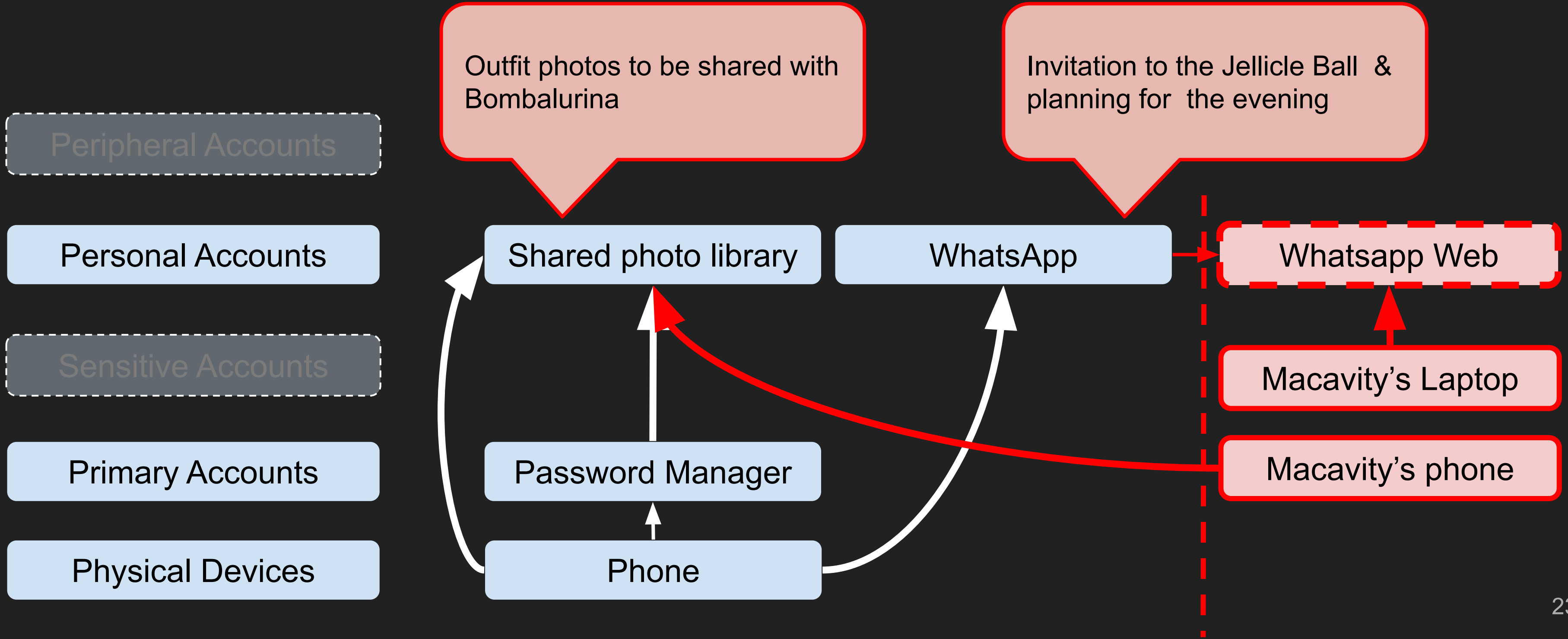
The Jellicle Ball

Jellicle cats come out tonight
Jellicle cats come one, come all
The Jellicle Moon is shining bright
Jellicles come to the Jellicle Ball



Macavity!!

Threat: Spying on photos and messages



Outfit photos to be shared with Bombalurina

Invitation to the Jellicle Ball & planning for the evening

Demeter’s Threat Model

Threat	**Mitigation**
Physical stalking during workouts	Stop sharing workout on Strava Set Privacy Permissions Change routes and routines
Tracking via Airtag/Smarttag/Bluetooth	Use notifications in iOS or Airguard on Android
Installing Stalkerware or “Spouseware”	Anti-virus, anti-stalkerware tooling, reset devices
Access to messaging apps on shared devices.	Log out all devices, rotate password, enable MFA ***Consider not sharing devices or access in the first place***
Continued access to photos including metadata	Revoke access to shared photo albums and backup services

Before acting: Consider the risk of escalation and violence!

Did Demeter do a good enough job?

She made a diagram of her digital life.

She went through that diagram systematically, thinking of threats.

She has things to do to mitigate those threats, or done those already.

Did Demeter do a good enough job?

- Considering:
  - Her abusive ex crashed the party
  - He abducted Old Deuteronomy
  - He attempted to abduct her
- But:
  - She found strength in numbers
  - Involved trusted friends

- Plan to fail: she had a back up

Journey to the Heavyside Layer

ever a cat so clever
istoffelees?

Touch me, it’s so easy to leave me,
If you touch me, you’ll understand what happiness is.

Up, up, up, to the Heavyside layer

Elevate your threat modeling:

A journey of understanding *over a security or privacy snapshot*

Continuous refinement *over a single delivery.*

The mystical divinity of unashamed felinity

Cats the Musical resources:

github.com/0xD4ni/cats

The ad-dressing of Cats

Questions?

Mastodon: dany@hsnl.social

LinkedIn: Daniëlle Wagemakers

Illustration: @ollie.v.oxenfree - Instagram

Now and Forever