



# How Threat Modeling Made Me Better at Online Dating

#DateSafe

# Who am I

- Security consultant, co-owner Revis Solutions
- Red teamer
- Teacher
- Anti: nihilism, security theater, wasted time
- Pro: risk based security
- Love chocolate chip cookies



Isaiah, 28

Entrepeneur

Chicago

# Who is this talk for?

People who want to...

---

Know what threat modeling is

---

Learn basic steps to do threat modeling

---

Apply threat modeling to development stages or end-user usage

---

Learn tips for online dating (regarding security)

---

Gain a basic understanding of

Data flow diagrams

STRIDE

Attack Trees

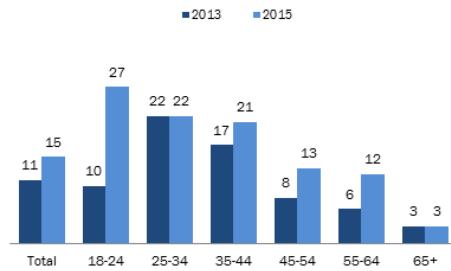
Principle ofnymity/linkability

# Technology and Dating

@isaiahsarju

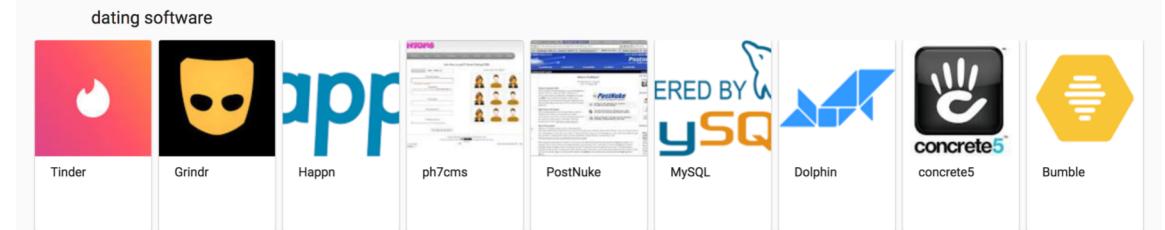
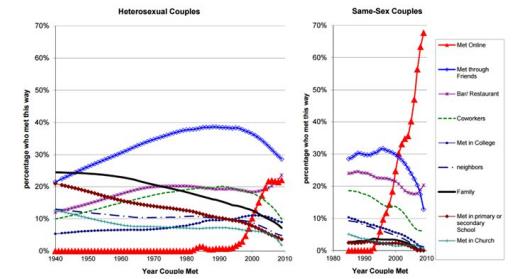
## Use of online dating sites or mobile apps by young adults has nearly tripled since 2013

% in each age group who have ever used an online dating site and/or mobile dating app



Source: Survey conducted June 10-July 12, 2015.

PEW RESEARCH CENTER



# Applications to Online Dating

Avoid

security nihilism

Promote

safe/positive interactions

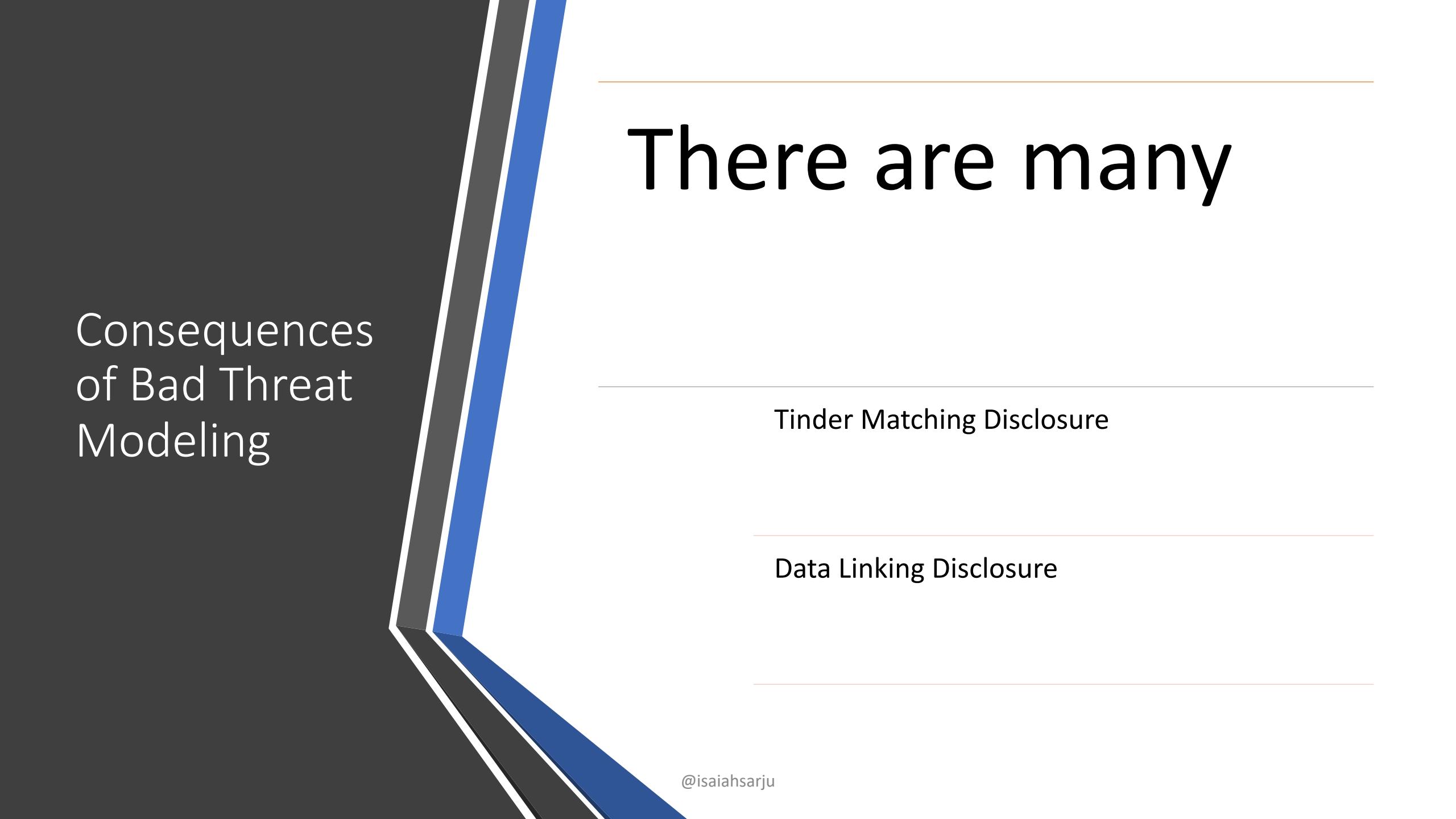
Build

more privacy/security centric applications

Protect

users:

- LGBTQ, Non-normative sexual/romantic preferences, People with disabilities, \_\_\_\_\_ minorities, (Everyone)



# There are many

Consequences  
of Bad Threat  
Modeling

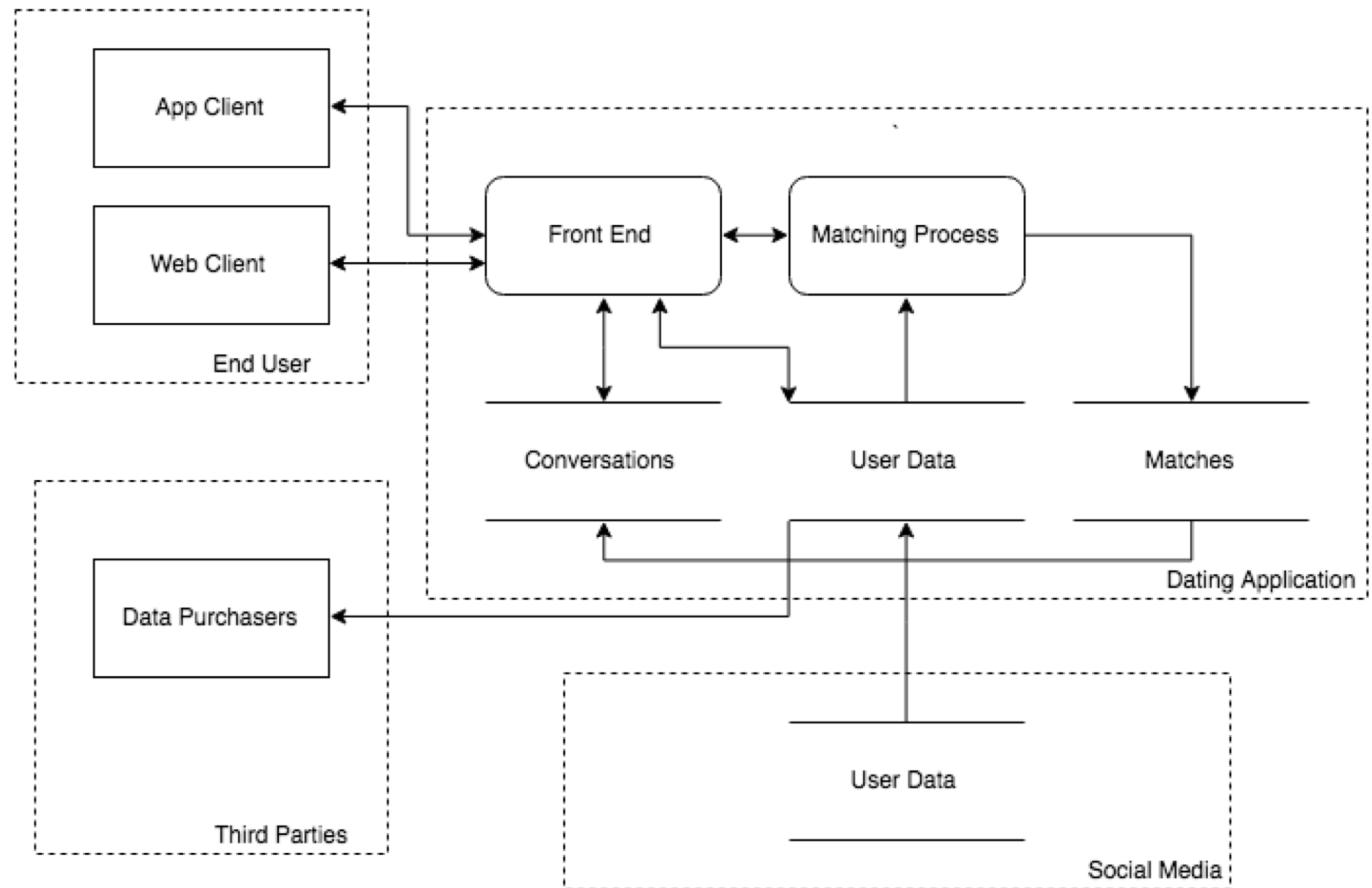
---

Tinder Matching Disclosure

---

Data Linking Disclosure

---



# Data flow diagrams

“Problems tend to follow the data flow,  
not the control flow” – Adam Shostack

---

Decompose application processes

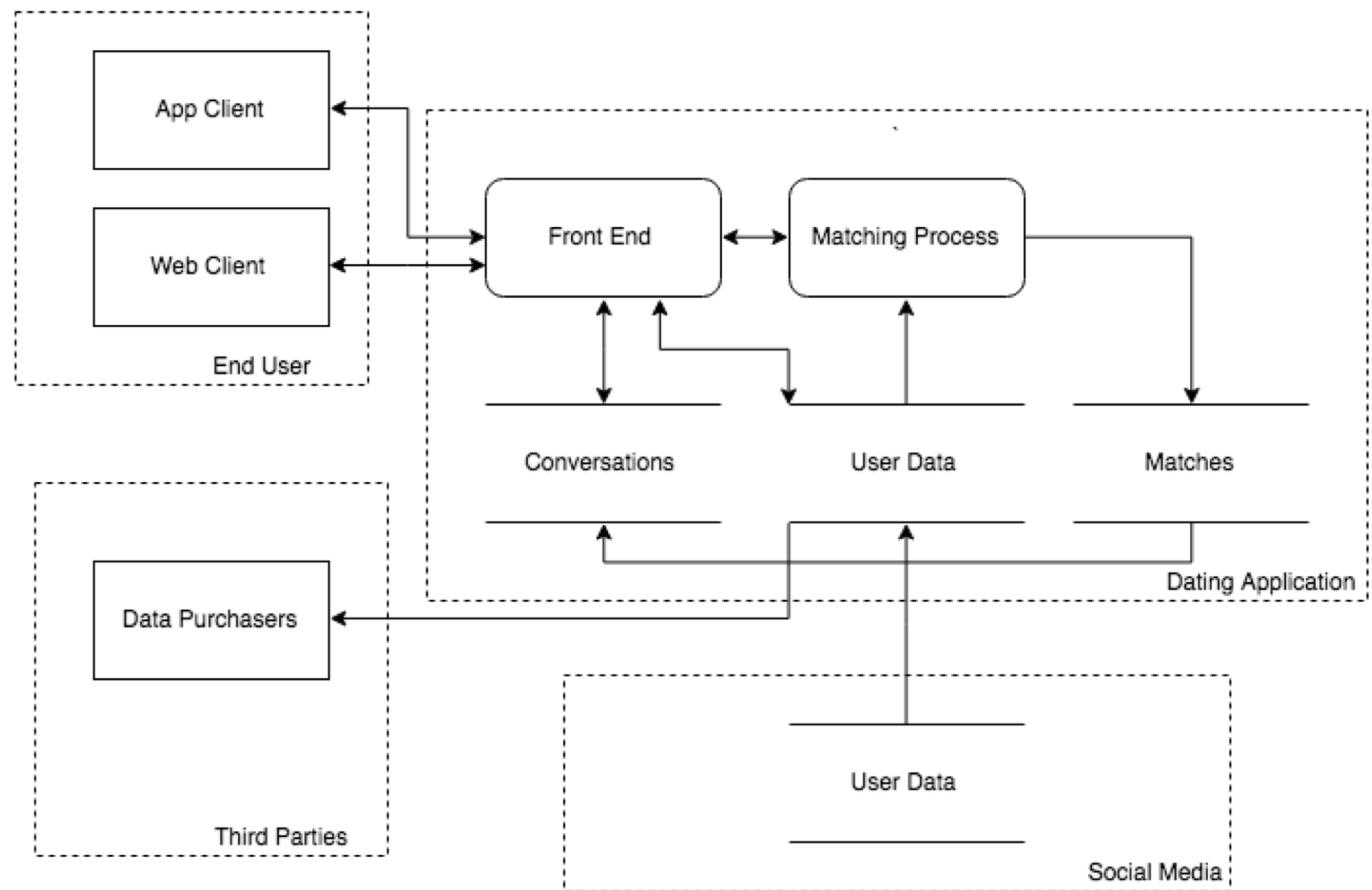
---

Understand data flow

---

Apply STRIDE to each step of the way

DFD



# Tinder Front End/Client Risk

---

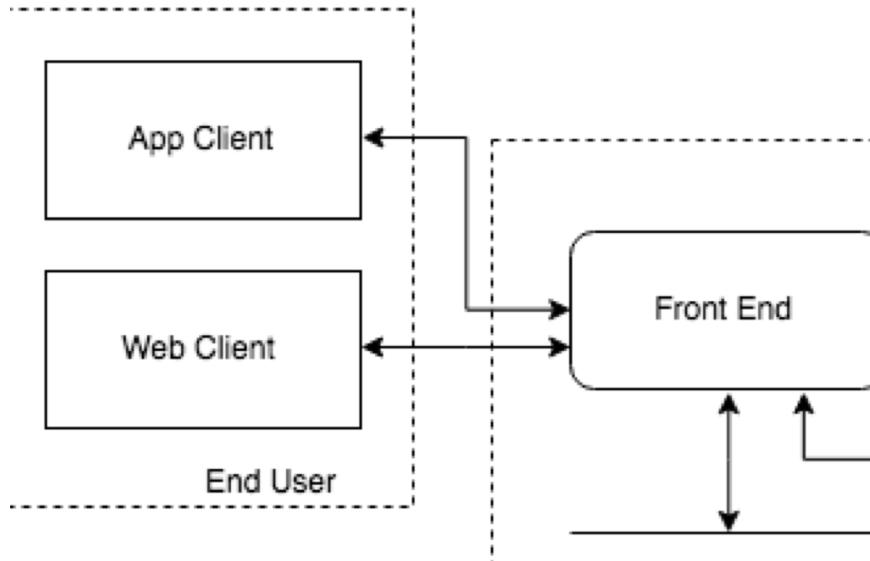
## STRIDE

## Example

<b>Spoofing</b> (Authentication)	Falsely claiming to be Isaiah Sarju on Tinder (Bumble offers “verification”)
<b>Tampering</b> (Integrity)	Changing a presented profile, changing a swipe
<b>Repudiation</b> (Non-repudiation)	“I didn’t swipe right on that person”
<b>Information Disclosure</b> (Confidentiality)	Disclosing swipe decision, disclosing matches/chats
<b>Denial of Service</b> (Availability)	Not able to connect to front end via client
<b>Elevation of Privileges</b> (Authorization)	Able to see profiles w/o matching, Facebook “view as” breach



C	SRC-PORT	DST	DST-PORT	SIZE	URL
2.168.8.13	50015	95.136.31.54	80	321	/59887a89b33bbdbd4ba2e9db/640x640_15f315c1-9f3f-4cd9-8e68-a6fc3
2.168.8.13	50015	95.136.31.54	80	321	/59887a89b33bbdbd4ba2e9db/640x640_15f315c1-9f3f-4cd9-8e68-a6fc3
87.57.193	443	192.168.8.13	49973	278	
2.168.8.13	50016	95.136.31.46	80	321	/59887a89b33bbdbd4ba2e9db/640x640_e90157b1-7566-46f6-881b-b7a1
87.57.193	443	192.168.8.13	49973	278	
2.168.8.13	50017	95.136.31.46	80	321	/55357ec85509b43422dc69ad/640x640_84b6c9b4-4561-4568-b63c-d2c
2.168.8.13	50018	95.136.31.46	80	321	/55357ec85509b43422dc69ad/640x640_96bde372-3f15-4558-966c-07cf
2.168.8.13	50020	95.136.31.46	80	321	/55357ec85509b43422dc69ad/640x640_f2950e00-b526-4d97-a52e-7751
2.168.8.13	50019	95.136.31.46	80	321	/55357ec85509b43422dc69ad/640x640_da0b71f1-e933-4490-8026-8fab
2.168.8.13	50021	95.136.31.46	80	321	/55357ec85509b43422dc69ad/640x640_eafdd0e3-8dd5-46ed-8a5c-f2f4
87.57.193	443	192.168.8.13	49973	374	
2.168.8.13	50023	95.136.31.46	80	321	/55ca572908e45e04415719ef/640x640_0a155395-b853-4f18-b7cf-67d7
2.168.8.13	50024	95.136.31.46	80	321	/55ca572908e45e04415719ef/640x640_9845d2fa-78ac-47b8-b820-9bb8
2.168.8.13	50022	95.136.31.46	80	321	/55ca572908e45e04415719ef/640x640_9c9e216b-3c55-4111-8d0a-4c87
87.57.193	443	192.168.8.13	49973	581	



# Tinder Information Disclosure (Checkmarx research)

# Risk Management Techniques

---

Acceptance

---

Avoidance

---

Transference

---

Mitigation/Reduction

# Risk Handling

---

**App**

HTTPs (mitigation)

Standardize response size  
(mitigation)

Don't care (acceptance)

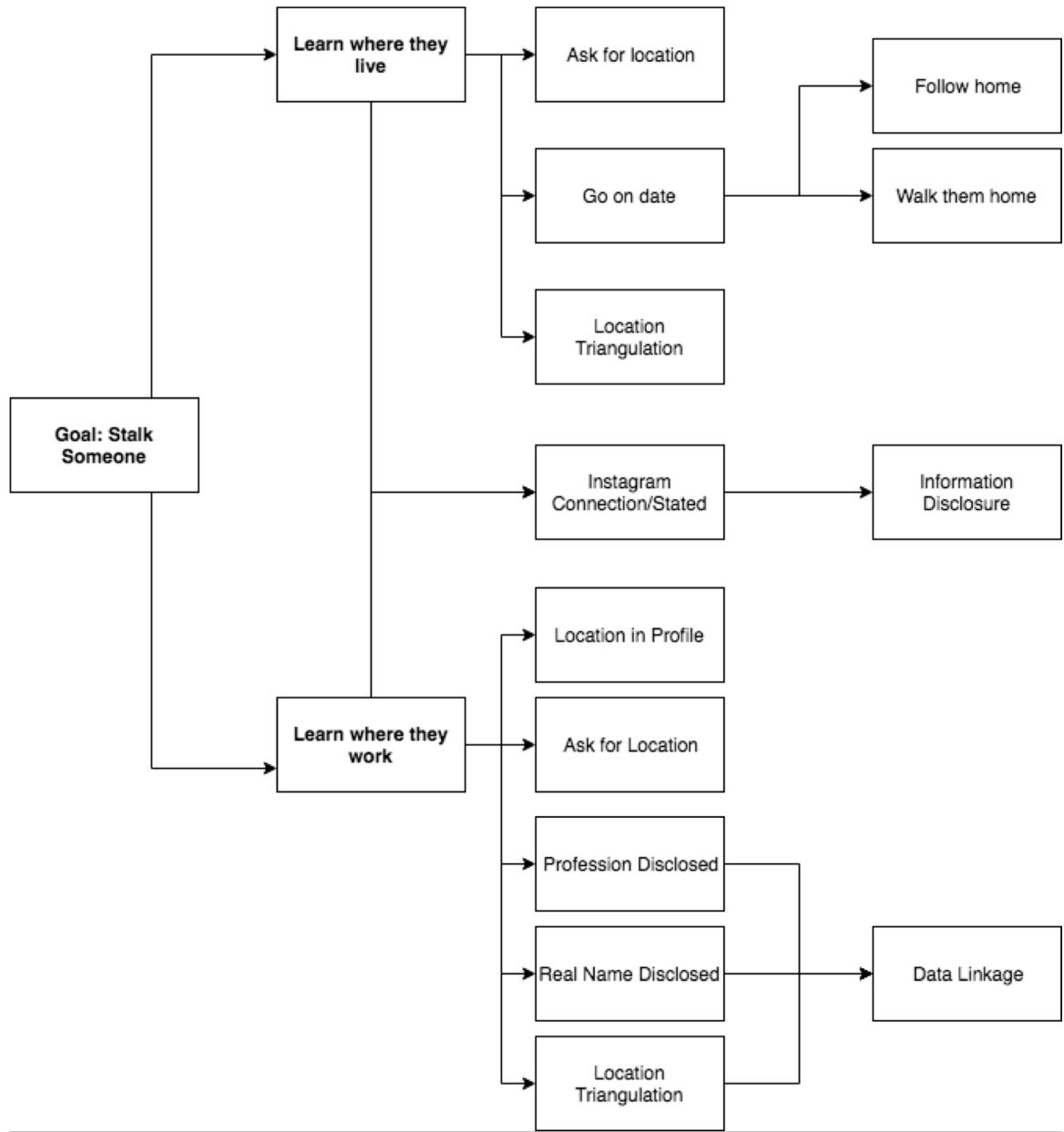
**User**

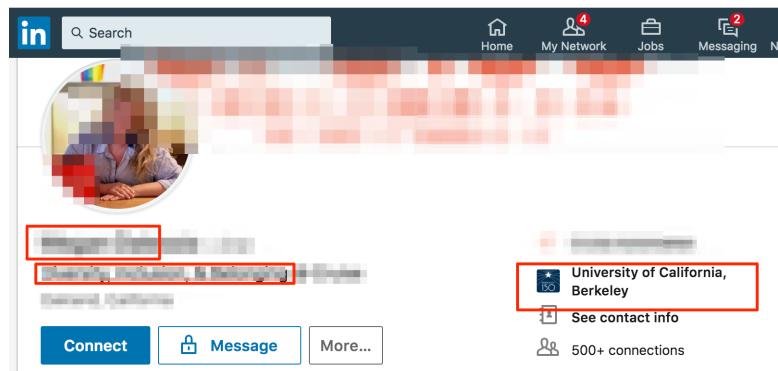
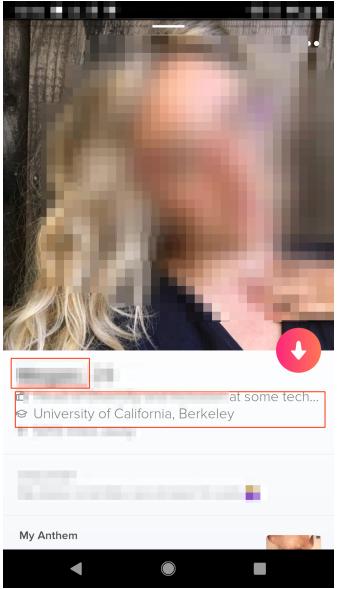
VPN (mitigation)

Only swipe at home (avoidance)

Don't care (acceptance)

# Attack Trees and Nyminity/Linkability





# Nymity and Linkability

---

- Nymity is the “amount of information about the identity of the participants that is revealed” – Ian Goldberg
- Linkability is the ability to bring one or more records together and combine information into a single record based on key(s) (virtual join)

# Risk Handling

---

App	User
Allow users to chose what information they disclose(transference)	Don't date (avoidance)
Don't disclose Instagram handle (reduction) (e.g. Tinder vs Bumble) <b>*Update</b>	Fake name (reduction)
Fuzzy/delayed location data (reduction) (e.g. Tinder vs Bumble)	Don't disclose employer (reduction)
Give users ability to hide distance (transference) (e.g. Tinder)	Don't connect Instagram (reduction) Prevent realtime location sharing (reduction) (iPhone vs Android)
	Don't disclose distance (mitigation) (e.g. Tinder)
	Spoof location (mitigation)
	Don't care (acceptance)

# My Love of Threat Modeling



---

Helps builders build better

---

Helps defenders think intentionally

---

Helps attackers prioritize attacks

---

Helps everyone make intentional decisions about data responsibility

# Sources

- Hergovich, Philipp and Ortega, Josue, The Strength of Absent Ties: Social Integration via Online Dating (September 14, 2018),  
<https://arxiv.org/pdf/1709.10478.pdf>
- Smith, Aaron, and Monica Anderson. "5 Facts about Online Dating." *Pew Research Center*, Pew Research Center, 29 Feb. 2016,  
[www.pewresearch.org/fact-tank/2016/02/29/5-facts-about-online-dating/](http://www.pewresearch.org/fact-tank/2016/02/29/5-facts-about-online-dating/).
- C. Fitzpatrick, J. Birnholtz and J. R. Brubaker, "Social and Personal Disclosure in a Location-Based Real Time Dating App," *2015 48th Hawaii International Conference on System Sciences*, Kauai, HI, 2015, pp. 1983-1992.  
doi: 10.1109/HICSS.2015.237, <http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=7070049&isnumber=7069647>
- Ghorayshi, Azeen. "Grindr Is Sharing The HIV Status Of Its Users With Other Companies." *BuzzFeed News*, BuzzFeed News, 3 Apr. 2018,  
[www.buzzfeednews.com/article/azeenghorayshi/grindr-hiv-status-privacy#.yp0J48W0N](http://www.buzzfeednews.com/article/azeenghorayshi/grindr-hiv-status-privacy#.yp0J48W0N).
- Nandwani M., Kaushal R. (2018) Evaluating User Vulnerability to Privacy Disclosures over Online Dating Platforms. In: Barolli L., Enokido T. (eds) Innovative Mobile and Internet Services in Ubiquitous Computing. IMIS 2017. Advances in Intelligent Systems and Computing, vol 612. Springer, Cham
- Duportail, Judith. "I Asked Tinder for My Data. It Sent Me 800 Pages of My Deepest, Darkest Secrets." *The Guardian*, Guardian News and Media, 26 Sept. 2017, [www.theguardian.com/technology/2017/sep/26/tinder-personal-data-dating-app-messages-hacked-sold](http://www.theguardian.com/technology/2017/sep/26/tinder-personal-data-dating-app-messages-hacked-sold).
- "Are You on Tinder?" Checkmarx, Jan 2018. [https://info.checkmarx.com/hubfs/Tinder\\_Research.pdf](https://info.checkmarx.com/hubfs/Tinder_Research.pdf).
- Shostack, Adam. *Threat Modeling: Designing for Security*. Wiley, 2014.



Q's

Help



@isaiahsarju