CS 5439:
Practicum in Computer Security

Fall 2018:

Tech Privacy & Safety in Intimate Partner Violence

Instructor: Tom Ristenpart
TA: Diana Freed

CORNELL TECH
HOME OF THE JACOBS INSTITUTE

Computer security

understanding and improving the behavior of computing technologies in the presence of adversaries

Attackers

Target/victim computing systems

Defenders (designers, engineers, lawyers, etc.)

Practicum: deeper dive into a practical computer security topic

Intimate Partner Violence (IPV)

CDC definition:

"Intimate partner violence includes physical violence, sexual violence, stalking and psychological aggression (including coercive tactics) by a current or former intimate partner (i.e., spouse, boyfriend/girlfriend, dating partner, or ongoing sexual partner)."

https://www.cdc.gov/violenceprevention/pdf/intimatepartnerviolence.pdf

NYC Hope webpage:

Physical, verbal, emotional, technological, sexual, financial, spiritual abuse stalking, isolation/extreme jealousy

https://www1.nyc.gov/nychope/site/page/recognize-abuse

Intimate Partner Violence (IPV) is a huge problem

IPV affects millions of people in the United States every year

25% of women
11% of men

suffered rape, physical violence, and/or stalking **by an intimate partner** at some point in their life

[National Intimate Partner and Sexual Violence Survey 2010-2012]
https://www.cdc.gov/violenceprevention/pdf/NISVS-StateReportBook.pdf

~360,000,000 Facebook users

~252,000,000 Android users

What role does technology play in IPV?

Tech abuse huge problem in IPV

[Southworth et al. 2005, 2006, 2007]

[Melander 2010]

[Dimond et al. 2011]

[Burke et al. 2011]

[Woodlock 2016]

[Matthews et al. 2017]

[Freed et al. 2018]

[Chatterjee et al. 2018]

Abusers exploiting technology:

- Harassing texts/messages
- GPS devices & spyware apps
- Victim accounts being “hacked”
- Physical device access
- …

Abuser Attacks Experienced		#Part.
Physical control	(a) Device/account controlled & monitored - Physical means	10
	(b) Device destroyed	4
	(c) Spyware installed	3
Cross-phase digital attacks	(d) Harassed online	8
	(e) Account hijacked - Impersonated	5
	(f) Account hijacked - Locked out	4
	(g) Account monitored - Remote or unknown means	2

15 participants --- Table from [Matthews et al. 2017]

New York City Family Justice Centers

Mayor's Office to Combat Domestic Violence

OCDV runs Family Justice Centers
One in each neighborhood of NYC

Range of services for domestic violence, sex trafficking, and elder abuse victims:

- Civil / legal services
- Counseling & safety planning
- NYPD
- District Attorney's offices
- Access to emergency shelter
- Non-profit organizations

Year-long qualitative study: methods

Clients (Survivors / Victims)	11 focus groups with 39 women (English & Spanish) ages 18-65 (average 42) from 15 different countries with range of education levels most no longer living with abusive partner
Professionals	Semi-structured interviews with 50 professionals female (45) and male (5) case managers, social workers, attorneys/paralegals, & police officers

“The reason that I came today is because I’m hoping to let people know my story. Maybe this is going to help somehow, to help another person who is going through the same thing.”

– Client

Client Story

[client story omitted for privacy reasons]

Four categories of common attacks

Ownership-based

- Abuser owns device/account
- Shared account/device
- Buying children device

- Prevent use / destroy device
- Digitally control access
- Track location, monitor usage

Account/device compromise

- Physical access to unlocked device
- Force password / pin revelation
- Remotely “hack” via security questions / passwords

- Install spyware / “dual-use” app
- Track location, monitor victim
- Steal or delete info
- Lock victim out of account
- Impersonate victim

Harmful messages or posts

- Call/text/message victim (from spoofed account)
- Post harmful content (e.g., threaten violence)
- Harass victim’s friends/family
- Proxy harassment

Exposure of private information

- Blackmail by threat of exposure
- “Doxxing” victim
- Non-consensual intimate images
- Fake profiles/advertisements of sexual services

"They'll hack into their phones and they'll hack into their accounts. Especially with intimate partner victimization." *– Case manager*

Threat models

Threat models specify:

(1) Who are Attacker and Victim
(2) Attacker's capabilities & goals

User 'Alice' who sets up account

Facebook
(or other web service)

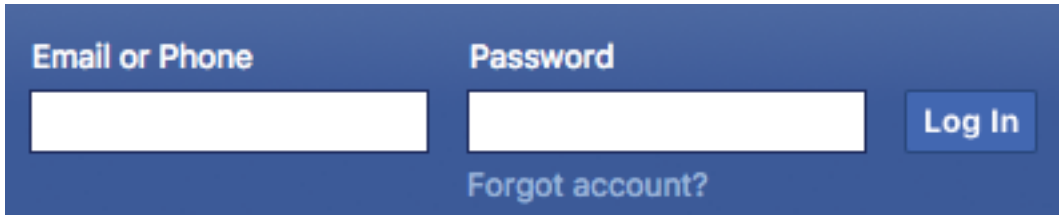
Remote adversary:

- Wants to login to Alice's account

Threat models

Threat models specify:

(1) Who are Attacker and Victim
(2) Attacker's capabilities & goals



Alice, sep1981

Alice, 123456

Alice, password

Alice, password1

User 'Alice' who sets up account and registers password

Facebook (or other web service)

Check that requests aren't from suspicious IP address

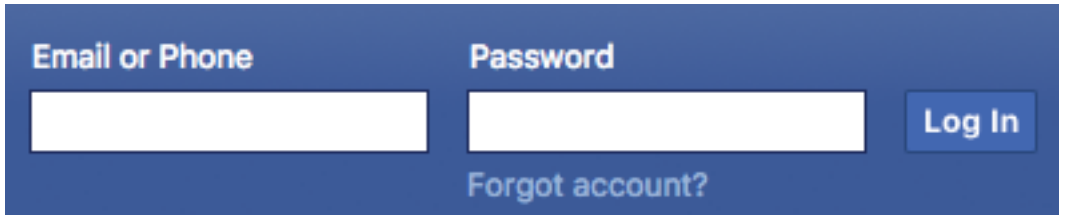
Remote adversary:

- Wants to login to Alice's account
- Knows typical passwords chosen by average users

Threat models

Threat models specify:

(1) Who are Attacker and Victim
(2) Attacker's capabilities & goals



Alice, sep1981

Alice, sep1981

User 'Alice' who sets up account and registers password

Facebook (or other web service)

Check that requests aren't from suspicious IP address

IPV adversary:

- Wants to login to Alice's account
- Knows Alice's password or compels disclosure
- On same network / computer as Alice

Threat models

Threat models specify:

(1) Who are Attacker and Victim
(2) Attacker's capabilities & goals

Most computer security defenses (mechanisms) are not designed for IPV threat models

Four categories of common attacks

Ownership-based

- Abuser owns device/account
- Shared account/device
- Buying children device

- Prevent use / destroy device
- Digitally control access
- Track location, monitor usage

Account/device compromise

- Physical access to unlocked device
- Force password / pin revelation
- Remotely “hack” via security questions / passwords

- Install spyware / “dual-use” app
- Track location, monitor victim
- Steal or delete info
- Lock victim out of account
- Impersonate victim

Harmful messages or posts

- Call/text/message victim (from spoofed account)
- Post harmful content (e.g., threaten violence)
- Harass victim’s friends/family
- Proxy harassment

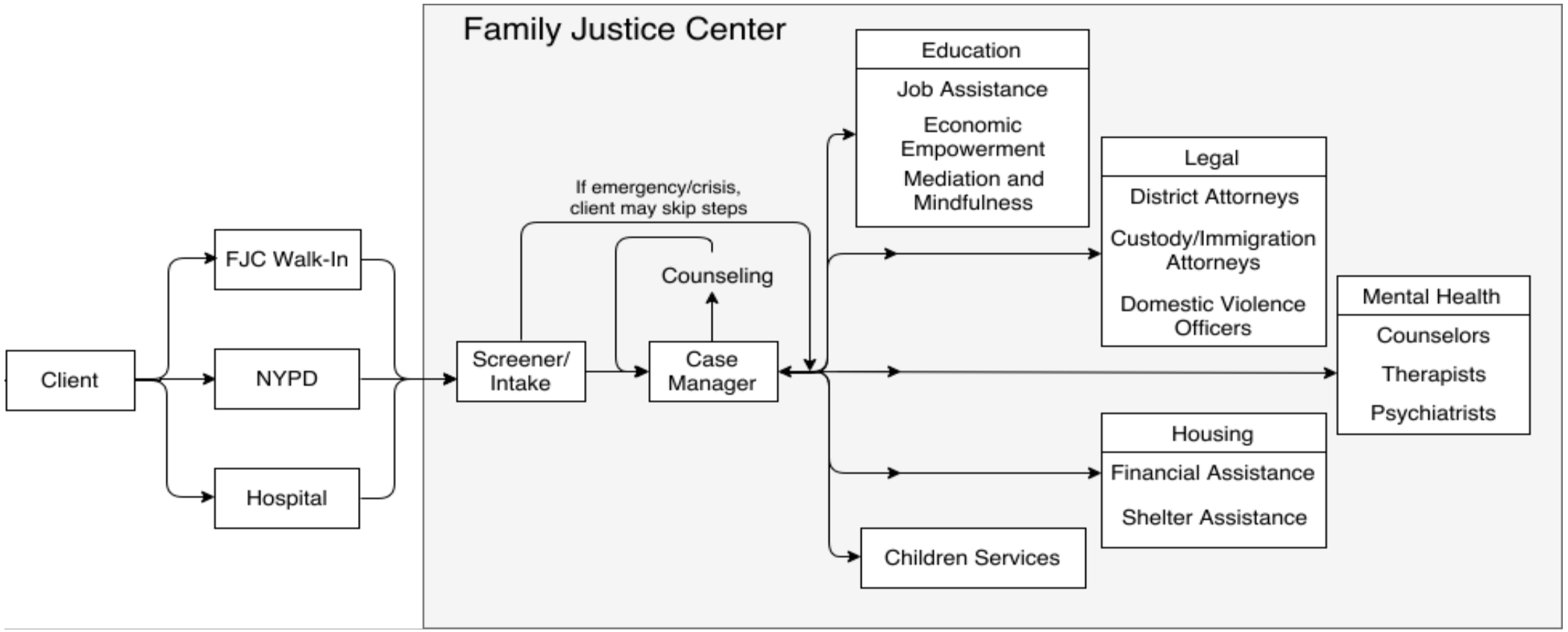
Exposure of private information

- Blackmail by threat of exposure
- “Doxxing” victim
- Non-consensual intimate images
- Fake profiles/advertisements of sexual services

Context of IPV undermines existing security mechanisms, which weren't designed for IPV threat models

Many non-technical issues as well

Clients and New York City Family Justice Centers



Number of technologists we met: 0

No best practices for evaluating tech risks

Victims, professionals feel they lack needed technology expertise

Victims overwhelmingly report having insufficient technology understanding to deal with tech abuse

"[The victim is] absolutely not savvy on technology."
– Case manager

Abusers usually considered to be "*more tech-savvy*" than victims

Professionals overwhelmingly report having insufficient technology understanding to help with tech abuse

"I end up Googling it. And then I'll deal with [the client]. But I think… I don't know how to do it so we'll just Google it together." – Case manager

"Google-as-they-go"

Tech advice tends to be general, not actionable

"You can choose who sees your Facebook activity either by setting a default setting under 'Privacy Settings' / 'Who can see my stuff' "

https://www.techsafety.org/resources-survivor/facebook/

Victims asked us repeatedly ***how to get to*** privacy settings for Facebook and on phones

Lack of ***actionable*** advice:
(1) Readily suggests a course of action
(2) Contains sufficient detail for recipient to act on it

Easier said than done: Visually documented tutorials? How to keep them up-to-date?

Complicated social context must be considered

"Delete your Facebook completely. Delete everything so he doesn't have access to you this way. Just throw away your phone and get a new phone."
– Social worker

Why can't you just:	Because:
Shut off contact with abuser	Legally obligated to communicate (shared custody of children)
Get new devices	Abuser pays for phones, family plan, and/or children's devices
Get off social media	Need it to get support from friends/family

Escalation a frequently mentioned complication

Abuse severity increases due to attempts by victim to block tech abuse

> "*Clients are much more at risk when they actually separate from their abusers because he suddenly no longer has any control over that victim. So often the only thing left is through the phone, so he's going to start harassing you, calling, texting. If you change your number, now he's most likely going to go crazy. So that's when he's going to start stalking you any way he can.*"
>
> – Social Worker

Some victims ***want*** (limited) communication to track state of mind of abuser

Legal and policy issue examples

(1) *"You have to figure out how to tie it all together besides the Facebook because if you don't have an order of protection, he's not violating so he's just harassing. That's when I ask the other questions and then maybe we can tie it into stalking … she can get her order of protection."* – Police officer

Abuse on Facebook not recognized as form of abuse that warrants an order of protection

Order of protection can legally restrict abusers from sending abusive Facebook messages

(2) *"The abuser made a fake Tinder account and put some really horrible explicit things and she was having tons, like upwards of like 25 people a night like ringing their doorbell. The abuser was corresponding with these people that wanted to hook up as if it was my client."* – Case manager

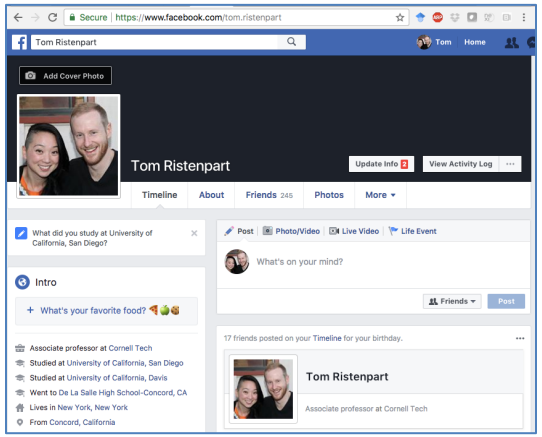
Heard about how in some cases it can be difficult to get "*come rape me*" style ads taken down because they are "*legally paid for*" by abuser

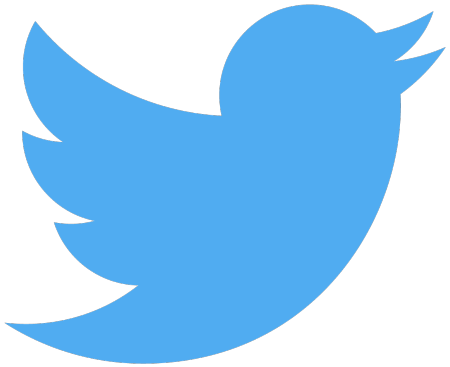
Summary so far

- Tech involved in many/most IPV situations
- Mismatch between security mechanism design and common IPV threat models
- Advocates, advice guides not always helping with tech issues
- Many social, policy, and legal complications

- Other settings with similarities with (and differences to) IPV:
  - abuse by family members/close friends/employers, bullying/harassment online, targeted attacks by Nation States against journalists/dissidents/etc., ...

Security practicum on IPV?





Goals:

- Learn more about computer security in practice, how to assess threat models and countermeasures
- Understand in detail how computer (in)security arises in IPV
- Understand how to improve design of technology and associated infrastructure to empower those working to stop IPV
- Help develop resources useful to advocates

Topics

- IPV “101” led by advocates from NYC OCDV
- Device monitoring and spyware
- Account compromise and recovery
- Internet of things
- Abusive content/messages
- Information disclosure (“doxxing”, non-consensual intimate imagery)
- HCI design to mitigate abuse
- Legal and policy issues
  - Guest lectures: Andrew St. Ana, Carrie Goldberg, Michelle Kaminsky
- Topics you want to hear about? Let me know

Resources

- Website:
  - https://github.com/cornelltech/CS5439-Fall2018
- Slack channel (you will be invited shortly)
- CMS
  - We may use for some homeworks
- IPVpedia
  - Private wiki on github will be used for many assignments
  - Goal will be to generate content usable by advocates

Intimate Partner Violence (IPV) not an easy subject

This class will involve some depressing content

Can always come talk to:

- Me
- Diana
- Jackie Klien (jk886@cornell.edu)

http://studentservices.tech.cornell.edu/nyc-health-resources/

Requirements

- 2 unit class
  - Less work than a 3 unit class
  - If elusive third unit is a big problem, let me know
- Participation:
  - Show up to all classes
  - Email Diana/myself if some issue arises and you will not make a class
- Readings:
  - Should be completed before class
  - Come ready to discuss
- Homeworks:
  - Homeworks typically due Sunday after they are assigned
  - Count equally towards grade
- May have extra credit opportunities towards end of class

Homework 1

HW1 is already up and assigned:

- Send Diana an email with your Github username

- Find an advice guide for IPV victims (each person should find a different one). Add an entry to the IPVpedia for it
  - May want to use Private Browsing Mode (will for future requests)
  - Think about what threat models are being addressed via the defenses. Do they seem aligned with an IPV threat?
  - How actionable are the suggestions in the guide?

- First reading for next week up too