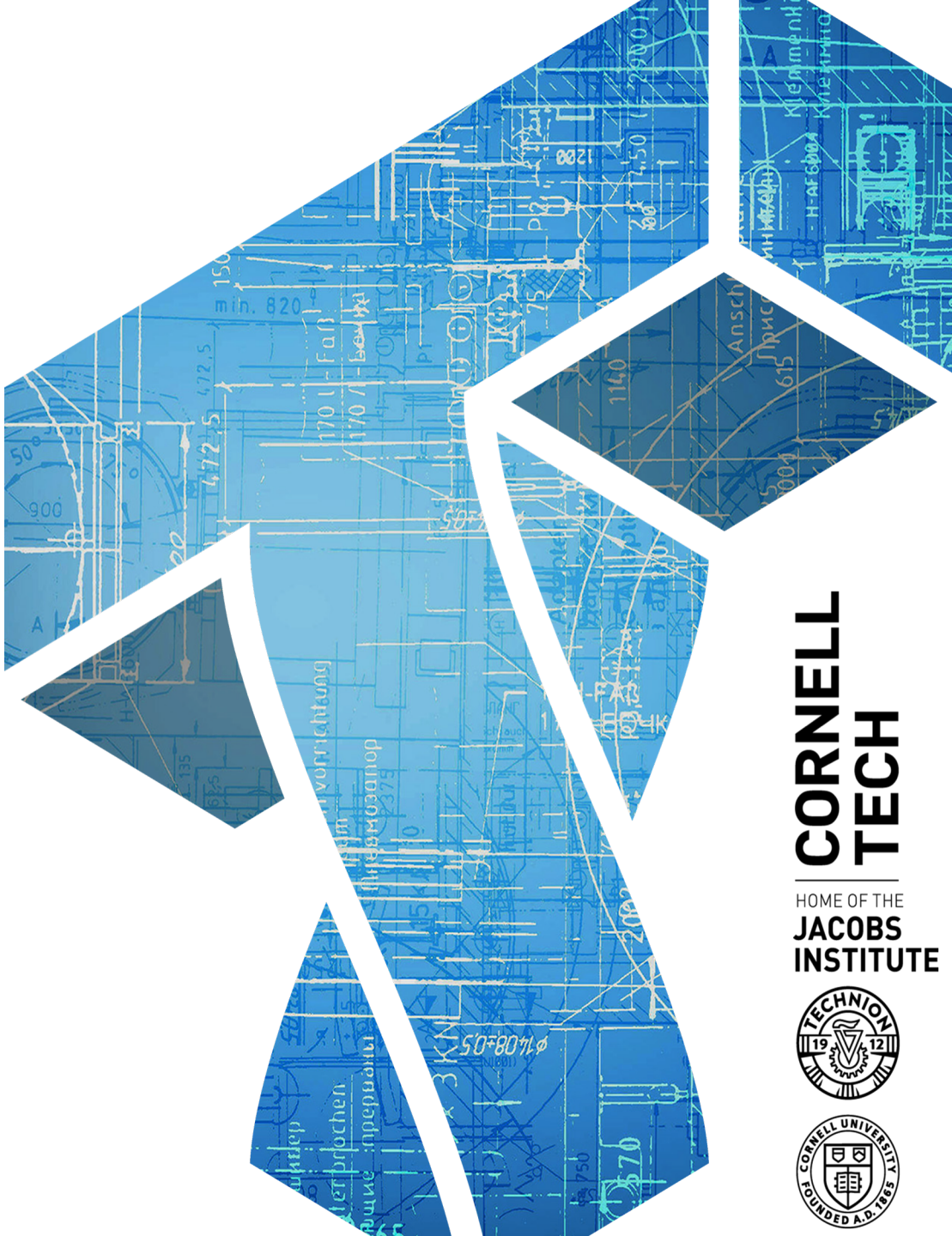
CS 5439:
Clinical computer security

Tom Ristenpart



CORNELL TECH

HOME OF THE JACOBS INSTITUTE

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

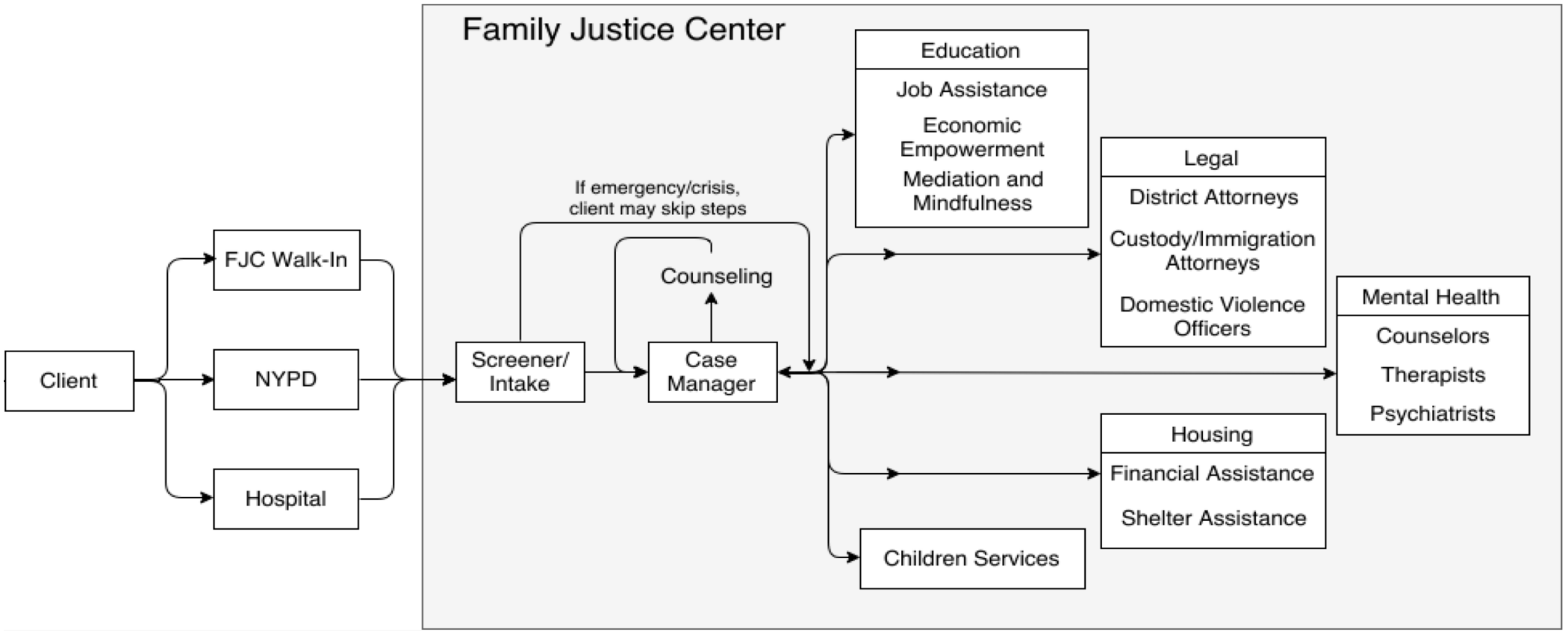
Harmful messages or posts

- 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

Clinical services for IPV victims



Clinical computer security

Technology volunteers (or professioinals) assisting clients with security issues via:

- Face-to-face consultation
- Technology investigations

How to recruit, screen, & train volunteers?

How to handle referrals and hand-off?

What tools are needed to perform investigations?

What legal protections are needed?

How do we evaluate outcomes?

How should consultations work?

This is work in-progress. What I'll discuss has not been validated yet!

Clinical models

Clinical models describe how to manage a clinic and deliver service

<u>Clinic model should include philosophy driving design</u>

- Client-centered approach (aka survivor-defined practice)
- Client's well-being and safety paramount

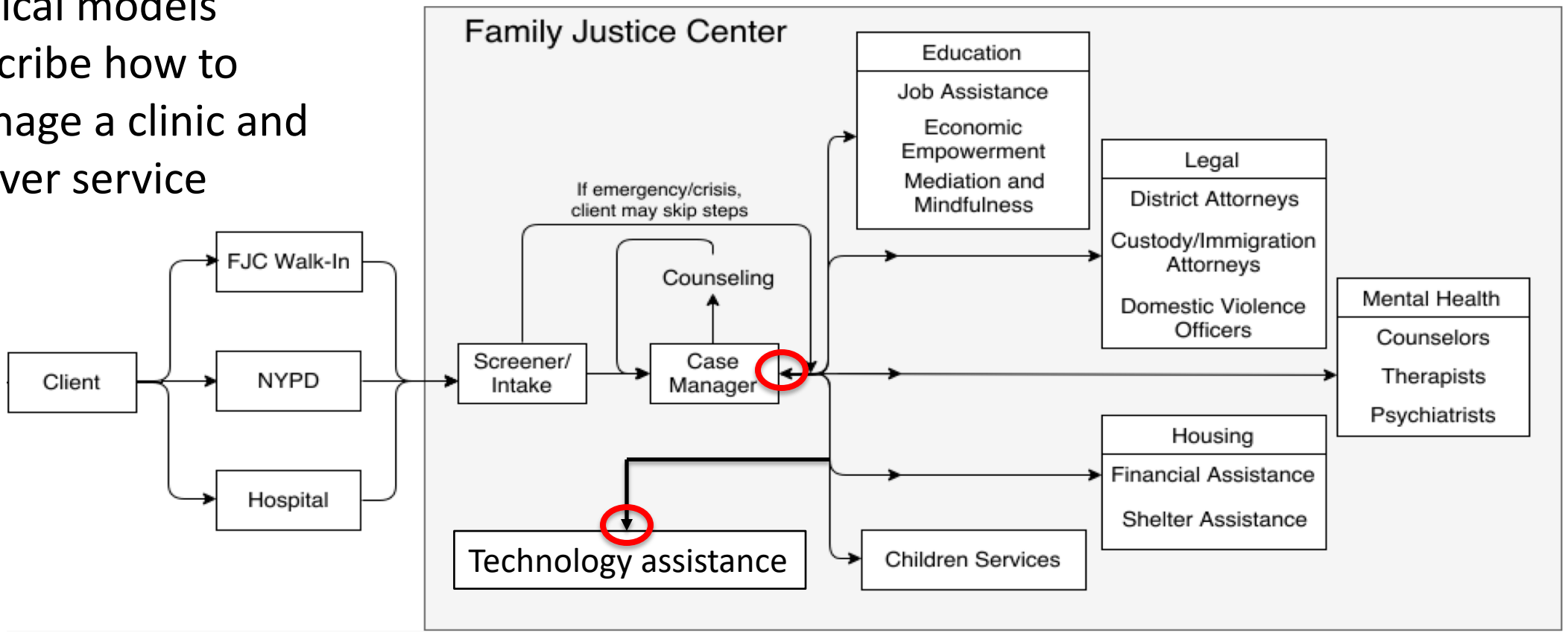
Technical tools must be used with appropriate care!

"At Safe Horizon, we believe that our clients are the experts in their own lives. We offer support, information, and expertise so that each client can exercise his/her right to make informed decisions and choose their own path. This **survivor-defined practice** is characterized by an emphasis on client choice, collaboration, and a sensitivity to the unique needs, risks, and resources of each individual."

https://www.safehorizon.org/programs/preliminary-results-of-the-client-centered-practice-evaluation/

Clinical models

Clinical models describe how to manage a clinic and deliver service



- Bootstrap off existing infrastructure
- Partner with existing non-profit or government organizations
- TECC clinic example

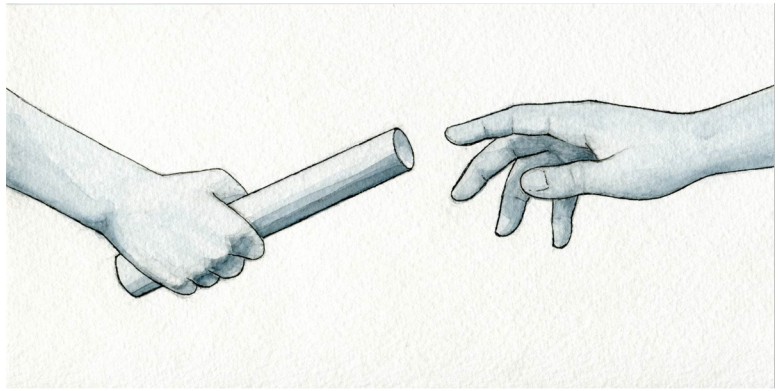
Referrals, hand-off, and managing roles

Part of clinical model is how clients end up being seen:

1. Referral-based treatment: Case manager or other professional refers client for a technology consultation
2. Walk-in treatment: Client can walk in to get technology consultation
3. Mixture

Hand-off is process of passing responsibility for helping client between professionals:

- Safety planning must take into account more than just technology situation
- Technology expert may not have information or be sufficiently trained to do safety planning
- Legal counsel may want evidence discovered by tech volunteer



Goals of tech consultation

Overarching:

- Provide information and support for client's technology issues
- Identify unrecognized technology issues

1. Identify chief concerns
2. Ascertain client's tech footprint and history
3. Diagnose threats
4. Provide information on remediations

Proposed consultation structure

1. Pre-consultation with referring advocate
2. Introductory safety procedures
3. Discussion
4. Investigation
5. Wrap-up
6. Follow-up

Pre-consult and safety procedures

Pre-consult:

- Overview consultation for case manager (or other professional)
- Mention safety planning handoff
- (Optionally) Gather some information on client
  - Requires client consent

Safety procedures:

- Devices may pose immediate risk to those in room, i.e., if they have spyware installed
- Currently planning on using faraday bags during initial discussion

Discussion phase

Discuss with client their technology concerns

- Map technology footprint (what devices? What accounts?)
- Identify entanglements (e.g., children's devices)
- Get a rough timeline (when was an account accessible to abuser?)

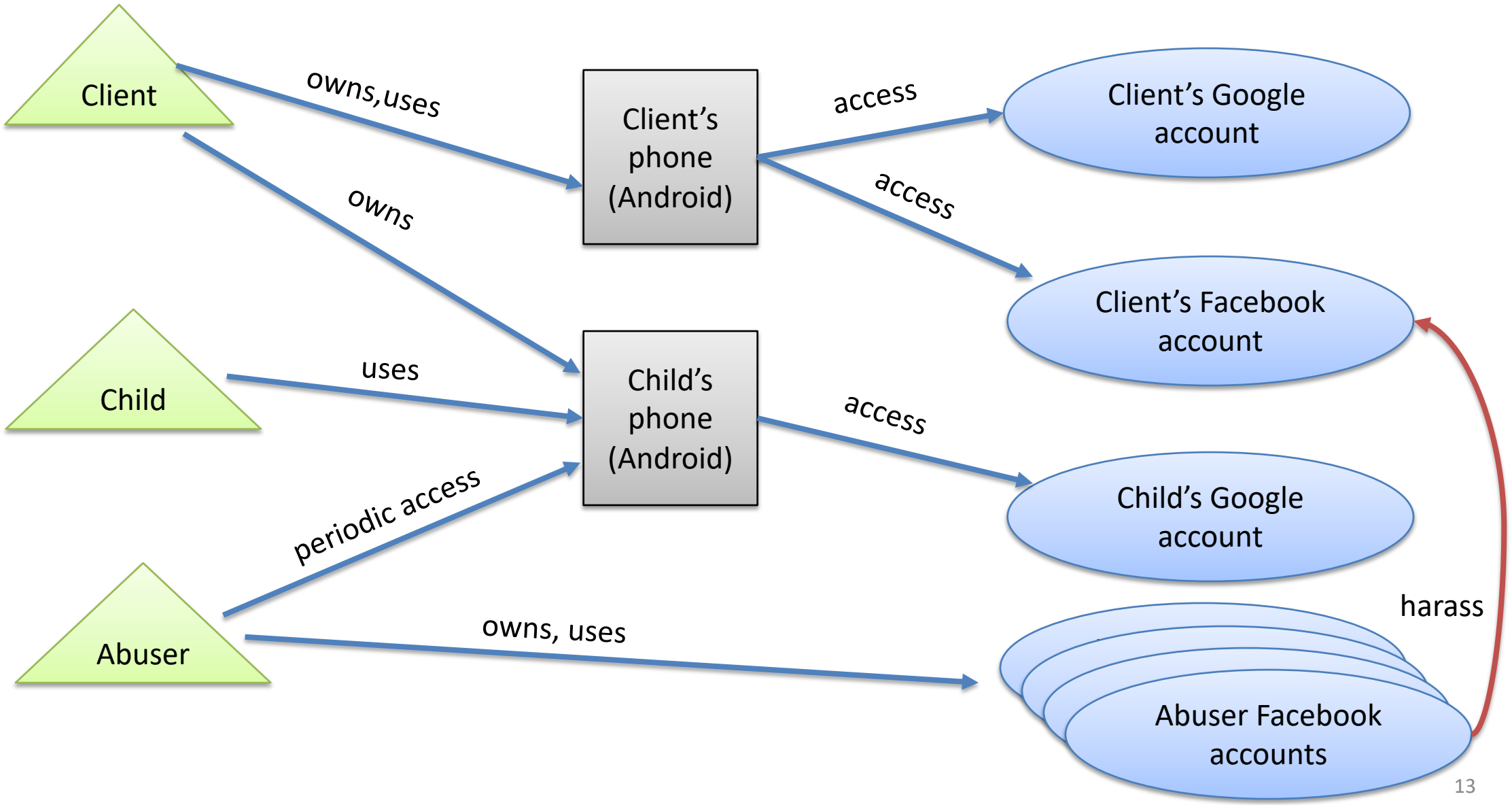
- Try to identify chief concerns
- Try to identify other potential risk factors
  - Can use instrument like TAQ-10
    - (Technology Assessment Questionnaire)

An example case

Carol has been suffering abuse for several years from her now ex-husband. After a few years of escalating sexual, emotional, and physical abuse, she recently left him and now lives in her own apartment with their 10 year old child. Carol received legal help from a local non-profit to obtain an order of protection legally barring him from contacting her, including physical contact and online messaging via social media. He does have monthly unsupervised visitations with their child. He works as an information technology engineer.

A year ago Carol saw on one of their credit card statements that he had purchased a product called FlexiSpy, which her lawyer said probably is some form of spyware that could monitor devices. She didn't know what he did with it, but assumed the worst and, after moving out, bought a new phone and tablet (for her child). Her lawyer helped her choose new passwords. To help remember all her many passwords she takes photos of the passwords and stores them on her phone. All this proved insufficient: she believes he's compromised one or more of her online accounts, and he recently used against her in court photos that he could only have gotten via illicit access to her Google account. She also often receives Facebook direct messages containing threats of physical confrontations from various fake accounts that are obviously him.

An example case



Investigations

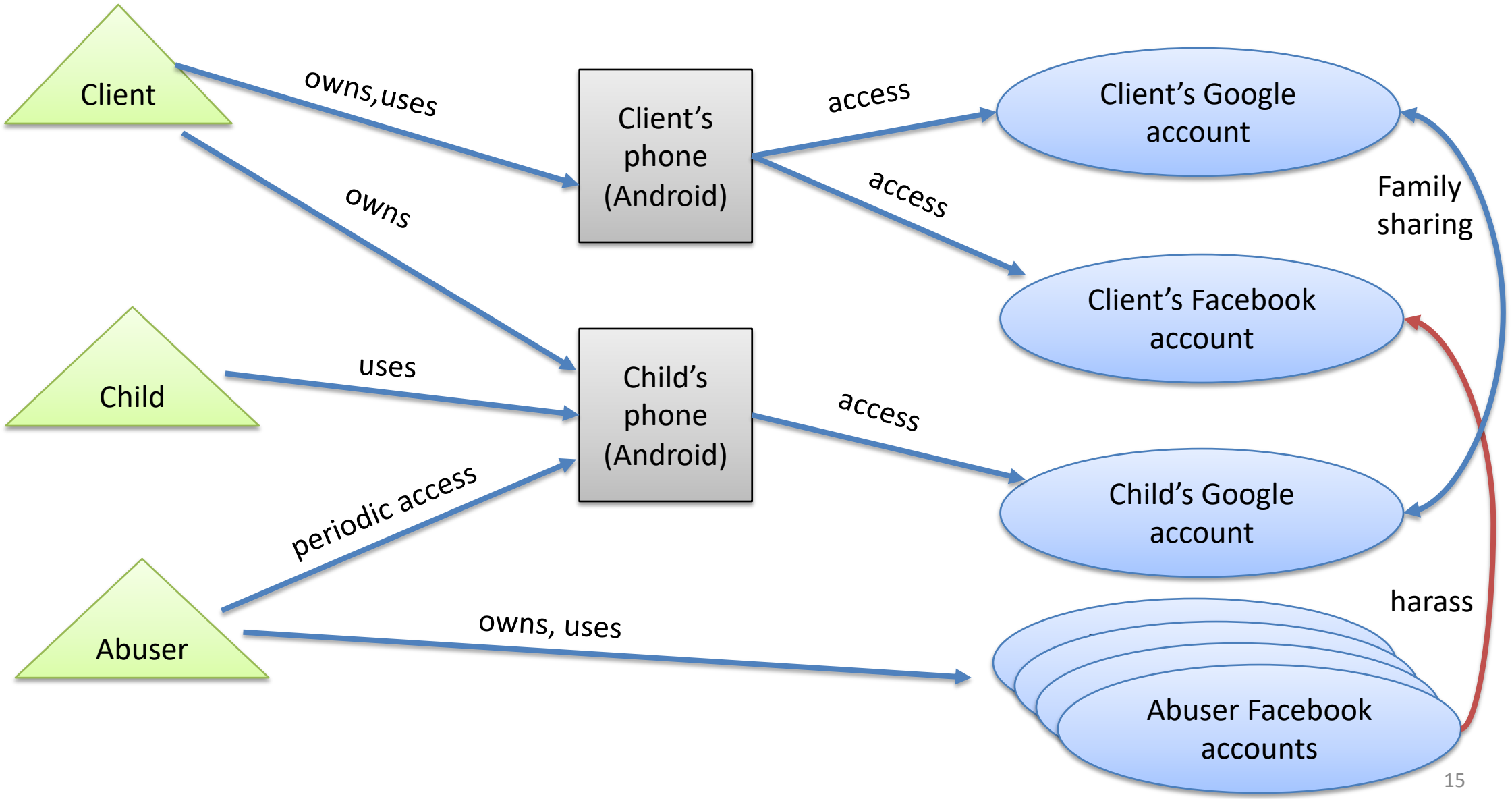
Tool-based investigations:

- Use spyware scanning tool to detect malicious software
- Wireless packet capture to flag spyware traffic

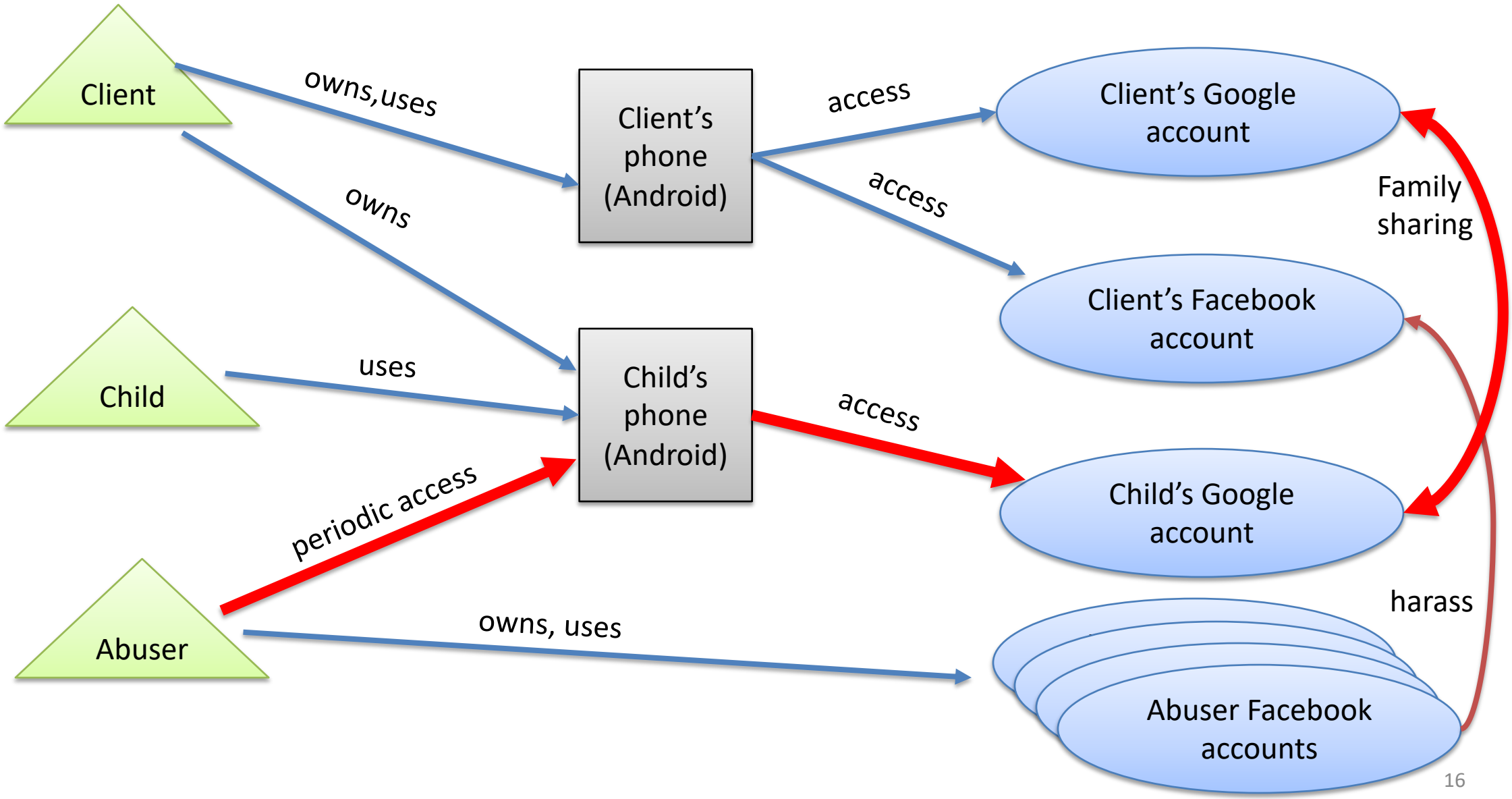
Manual investigation:

- Show client how to check various configuration settings manually
  - Example: Google account settings, recent logins, etc.

An example case



An example case



Wrap-up and follow-up

Provide information on possible remediations in wrap-up

- Should not be prescriptive
- Any remediations *must be safety planned*
  - Example: Turning off family sharing will be noticed by abuser next visit with child
  - Example: Discuss privacy settings on Facebook, and blocking mechanisms
- Handoff to case manager by explaining remediation and relevant information for safety planning
- Try to leave client feeling empowered

Follow-up

- Some issues may not have obvious solutions, can promise to do some research into it and get back to client

Proposed consultation structure

1. Pre-consultation with referring advocate
2. Introductory safety procedures
3. Discussion
4. Investigation
5. Wrap-up
6. Follow-up

We are currently field-testing this type of consultation structure in our research

Clinical computer security

Technology volunteers (or professioinals) assisting clients with security issues via:

- Face-to-face consultation
- Technology investigations

How to recruit, screen, & train volunteers?

How to handle referrals and hand-off?

What tools are needed to perform investigations?

What legal protections are needed?

How do we evaluate outcomes?

How should consultations work?

Hypothesis: other contexts beyond IPV that would benefit from this approach