1 | Previously, on Computer Security

How *do* we protect user data?

Increased security always comes with a trade-off of ease of use.

1.1 | Lessons from the number game

- Security is hard :(
- Security is hard; uncertainty of security makes it harder
- Its easier to brainstorm attacks than to brainstorm solutions

2 | Threat Modeling

Thread modeling is a fancy way of creating a structured brainstorming framework.

2.1 | Seven Questions to Threat Modeling

- Specifically, what are we protecting?
- Who are we protecting it from, and what are their motivations?
- What methods of attack do we prevent? What are types of attacks that we don't prevent?
- What are the possible effects of these attacks? ("What types of attacks do we prevent, and how does that play on what we are protecting?")
- What are the resources of attackers?
- What are our resources?
- What should we do?

2.2 | Actual Threat Modeling for Facebook Health Communities

…that Wes did.

2.2.1 | What are we protecting?

Health Communities use Facebook Groups to connect people around the world who have share health conditions. These groups are created and run by Facebook users and offer emotional support and information.

Goal is to protect the users of these groups from physical and emotional harm.

Goal is *not* protecting Facebook itself.

2.2.2 | Who are we protecting it from, and what are their motivations?

1. Protecting From…
    - Profiteers who are looking to exploit vulnerable populations (e.g. scam artists, quacks)
    - Well-meaning but misinformed users
    - Trolls trying to get emotional reactions for funzies
    - Insurance companies who might change user premiums
2. Not Protecting From…
    - Facebook employees
    - Hackers who are not Facebook users (i.e. national states)

2.2.3 | What methods of attacks do we prevent?

- Selling or trading drugs/equipment on Facebook
- Misinformation, either malicious or well-intentioned, that leads to physical harm
- Bullying
- Privacy leaks: somehow, someone's data from these groups leaks:
    - By malicious actors…
    - By Facebook itself…
    - By users themselves…

2.2.4 | What are the possible effects of these attacks?

1. Physical harm to users
2. Loss of trust in the platform (Facebook)

2.2.5 | What are their resources of the attackers?

Believe that attackers' resources are limited:

- Profiteers will only spend resources if the reward is worth it, so very little
- Well-meaning users will spend little resources, or none if educated
- Trolls will find an easier target to attack
- Insurance companies are a question mark: lots of resources for high reward

2.2.6 | What are our resources?

Surprisingly limited, in some cases:

- 3 engineers, no PM, and half a data scientist
- No medical experiences

But surprisingly large:

- Multi-bullion dollar company
- Dedicated security, misinformation, bullying, and illegal sales teams
- Secret weapons: group admins and a direct line to Mark Zuckerberg

2.2.7 | What should we do?

1. Align closely with the Groups team as a whole
2. Partner with dedicated teams
3. Build/own ONLY the things that the group specifically care about
   (a) Sellling => Illegal Sales Team
   (b) Misinformation => Misinformation Team
   (c) Bullying => Well-being Team
   (d) Privacy… a point of focus

Hence, the first feature is allowing real-name users to post anonymously.