EN.601.741

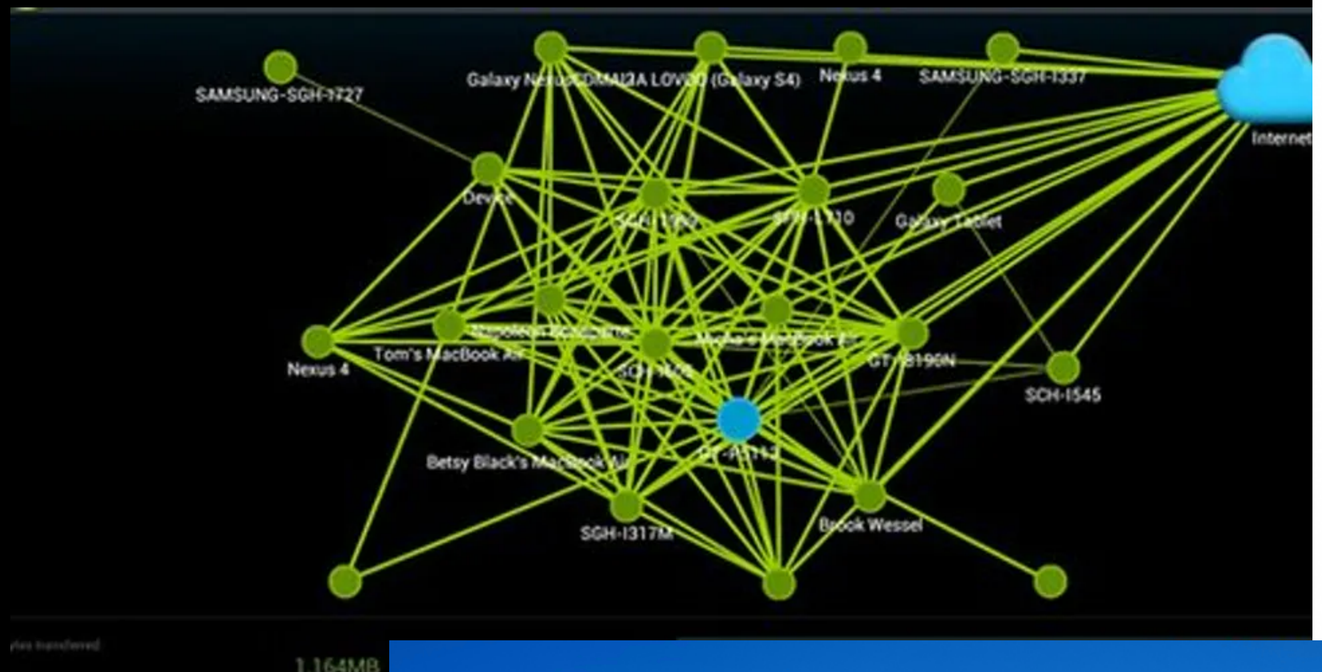
Advanced Topics in Secure and Censorship-Resistant Communications

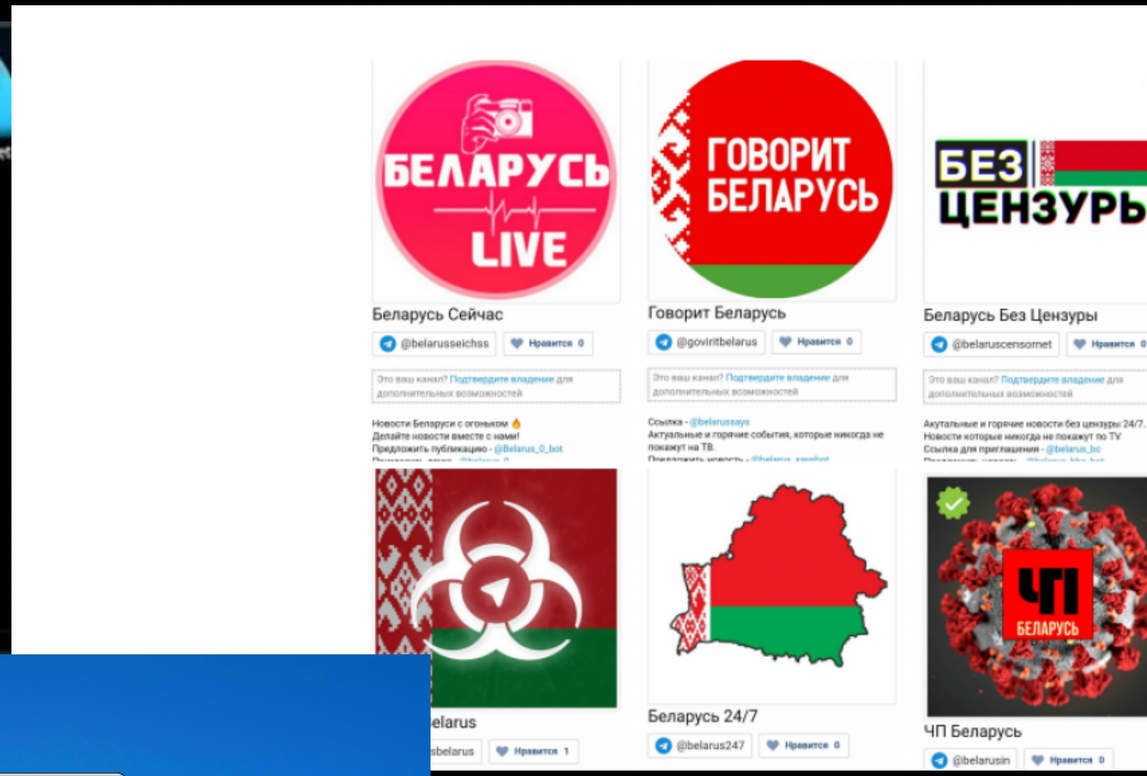
Instructor: Matthew Green
Spring 2021

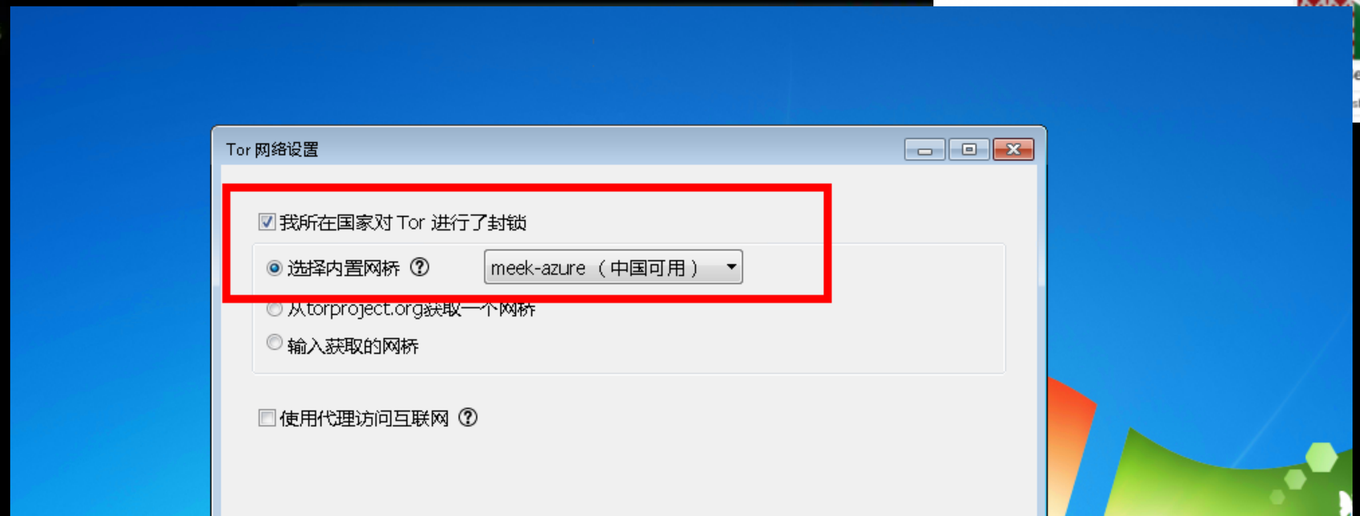
What is this class about

What is this class about

What is this class about







What is this class about

How to Stop Signal From Telling You When Your Contacts Join

CHRIS HOFFMAN @chrisbhoffman

JAN 8, 2021, 5:51 PM EST | 1 MIN READ

What is this class about

Facebook At Center Of Storm Over Child Sexual Exploitation

March 17, 2020 / ***Michael Passoff***

There has been an explosion of child sexual abuse ma
companies take more aggressive action. What was
has–through the proliferation of smart phones, socia
internet and **children going online.** (One third of In

Twenty years ago, there were about 3,000 reports
increased to more than 100,000 reports. By 2018,
images and videos. Experts lament that this is just th

In 2018, Facebook (especially **Facebook Messenger**
CSAM (91 percent of the total). To be fair, Facebo

JUSTICE NEWS

Attorney General William P. Barr Announces the Launch of Voluntary Principles to Counter Online Child Sexual Exploitation and Abuse

Washington, DC ~ Thursday, March 5, 2020

Remarks as Prepared for Delivery

Good afternoon. I am pleased to be joined here today by Acting Secretary Wolf of the U.S. Department of Homeland Security, distinguished colleagues from Australia, Canada, New Zealand, and the United Kingdom, and representatives from leading tech companies, to announce a very important initiative: Voluntary Principles to Counter Online Child Sexual Exploitation and Abuse.

Last summer, I traveled to London for the Five Country Ministerial Digital Industry Roundtable. There, our five nations met with senior representatives from Facebook, Google, Microsoft, Roblox, Snapchat, and Twitter. We agreed that a more robust global response to online child sexual abuse was necessary to ensure that all children across the globe are protected, and that there is no safe space online for offenders to operate. Further, we committed to developing a set of voluntary principles to ensure online platforms and services have the systems they need to combat online child sexual exploitation. As a result of that meeting and much diligent work since then, today, we are collectively launching the 11 Voluntary Principles. I am happy that our hard work has come to fruition with today's event.

What is this class about

- This is a course on cryptography and computer security
  - But it is not only about those things
  - It is primarily a course about communication, and figuring out how we can improve communication — in a regime where others don't want it
  - This is cross-disciplinary
  - We will need to reason about what's needed, what works, what doesn't, how people respond to it

Topic areas

- Encrypted messaging
- Anonymous communications networks
- Censorship-resistant publishing and networking
- Ad-hoc networking (e.g., mesh networking)
- Disinformation
- Private reputation systems

Topic areas

Encrypted messaging

- Encrypted messengers are taking over the world
  - Many people think this is a bad idea, and would like to stop it
  - The battle to slow encrypted messaging has taken some turns recently, and we're going to talk about that (me on Weds)
  - So much tech here, we're good at encrypted messaging: except where it's blocked
  - Which is a big part of the world!

Topic areas

Censorship-resistant comms & publishing

- Nation-state attackers are getting better at blocking the Internet
  - This breaks down into “dumb” blocks (Belarus) and “smart ones” (GFW)
  - We should care about both
  - Many techniques trying to deal with this:
    - Steganography of various forms (e.g., decoy nets, bridges)
    - Telegram proxies in Belarus

Topic areas
Ad-hoc networking

- How do you organize a protest when the networks are down?
  - This is not a small problem, see e.g., Belarus, Hong Kong
  - For years people have talked about using ad-hoc and mesh networks to deal with these situations
  - Finally they’re being deployed (see Hong Kong)
  - Results are mixed, security results are highly problematic

Topic areas

Anonymous communications and networking

- Anonymous communications breaks into several areas
  - Anonymous low-latency network comms (e.g., Tor)
  - Anonymous high-latency network comms (e.g., Mixnets, DCnets)
  - Relatively few of either of the latter technologies actually deployed, and Tor under threat
  - Many questions about how to prevent abuse on anon-comms networks (e.g., PrivacyPass)

Topic areas
Disinformation

- This is outside of the usual domain of problems but it matters a lot
  - Is there anything at all we can do as cryptographers here?

Topic areas

Reputation

- Can we combine privacy with abuse reporting and reputation
  - Reputation systems exist, can we use them to prevent abuse?
  - Does any of this make sense?

This course will have opinions and biases

- This is a fraught and political area, and we shouldn’t pretend that it isn’t
  - This is a U.S. university and largely a group of U.S. students
  - Even within the U.S. we have plenty of political disagreements
  - There are active questions right now about the tradeoff between free speech and misinformation
  - Anything that helps privacy and censorship resistance also admits some pretty awful behavior (CSAM)

Political considerations

- In the past I've always taken the view that "more speech is better", and anything that makes speech easier and harder to trace must be good
- Events of recent years have made me question whether this is always true
  - I want to believe, though
  - There are some hard questions in here, and I don't propose to answer them. But you might have to.
  - You (more than ever now) may find yourself empowering speech you strongly disagree with. Speech that may get people hurt.
  - I would love to tell you that technology will somehow fix this.

Boring logistical stuff

- Our goal is to find research topics
  - Thus the course will be divided into three areas:
    - Presentations
    - Discussion
    - Project work <- Most of your grade

Presentations

- Once per week a full presentation on a technical topic area
  - This is not just a presentation about one research paper
  - For example, say we want to know everything that is happening with decoy routing
    - This is a topic area that was invented a decade ago, there are dozens of papers, so what is it, what's going on with deployment today
    - **Most critically: does it work?**
      If not, what are the open problems with it?

Course resources

- Course website:
  https://github.com/matthewdgreen/censorship
- Piazza (easy way to distribute materials)
  https://piazza.com/class/kkcraxd04rz76a (search this course #)
- **We will use a Telegram group to communicate course updates**
  Please sign up and email me your numbers
  (if you don't want to upload your personal phone number to Telegram or me that's understandable, make a Google Voice account and get a phone number from there.)

Course plan going forward

- Today: let’s introduce ourselves and discuss interests
  (we will end early today)
- Wednesday: I will present on e2e messaging
- Monday: discussion of the previous week and a follow-up presentation
  (I would like to switch off this cadence to reverse M/W)
- Next week: decoy routing
- Guest lectures (so far)
  - 2/1: Cecylia Bocovich & Philip Winter - Tor bridges

Project deliverables

- 2/15: Figure out what you’re interested in and propose it
- 3/8: Project midterm report
- 4/8 Project update
- 4/29 Project due