



Advanced Network Security

Lecture 1: Introduction

Harald Vranken, Katharina Kohls

08.09.2022

Open University Nijmegen

Radboud University Nijmegen



Dr.ir. Harald Vranken

- ▶ Associate professor at Open Universiteit
- ▶ 1 day/week at Radboud University
- ▶ ✉ harald.vranken@ou.nl
- ▶ ℗ harald.vranken
- ▶ 🌐 www.open.ou.nl/hvr

Internet and Web Security



Dr. Katharina Kohls

- ▶ Assistant professor at Radboud
- ▶ kkohls@cs.ru.nl
- ▶ [katharina.kohls](https://www.linkedin.com/in/katharina-kohls/)
- ▶ kkohls.org

Mobile Network Security

Course Content

1	Introduction	08.09.2022
2	Mobile Networks	15.09.2022
3	3 Attacks on L2	22.09.2022
4	ReVoLTE Attack	29.09.2022
5	4G and 5G	06.10.2022
6	5G SUCI Catcher	13.10.2022
7	Presentations 1	20.10.2022
<hr/>		
8	WiFi Security 1	10.11.2022
9	WiFi Security 2	17.11.2022
10	Botnets and DDoS	24.11.2022
11	Routing Security, BGP, DNS over HTTPS 1	01.12.2022
12	Routing Security, BGP, DNS over HTTPS 2	08.12.2022
13	Presentations 2	15.12.2022
14	Wrapup	22.12.2022

Structure:

- ▶ Topics follow the content of the lectures
- ▶ Work in groups
- ▶ Pick a topic for the presentations
- ▶ Project is worth 1 EC

Grading: 5/6 exam + 1/6 project



Why projects?

- ▶ Get hands-on experience
- ▶ Do practical stuff (programming, measuring)
- ▶ Related to the lectures

Why presentations?

- ▶ Practice!
- ▶ Do your own wrapup

What will be the format?

- ▶ Online exam on Cirrus
- ▶ Mostly knowledge questions
- ▶ Everything close to the lectures

Exam: 18.01.2023 12:45

Brightspace is the answer:

- ▶ Before each lecture, we upload the next set of slides there
- ▶ Homework assignments will be uploaded here
- ▶ Use the discussion forum!

Activities → Discussions

Course Home Content Activities ▾ Administration ▾ ePortfolio Help ▾

Discussions

Settings

Help

Discussions List

Subscriptions

Group and Section Restrictions

Statistics

New ▾

More Actions ▾

Filter by: Unread Unapproved

▼ Collapse All Forums

Questions and Discussions ▾

Please share your questions and thoughts here so that everyone can benefit!

Topic	Threads	Posts	Last Post
General Questions Regarding the Course ▾ Everything that in general is related to the course	0	0	
Questions Regarding Lectures ▾ If something remains unclear, if you have further questions, if you are looking for resources or examples, ...	0	0	

Motivation

Safety vs. Security

Safety and Security are both about protection, still different:

Safety: against (unintentional) accidents or disasters

- ▶ anticipate what can go wrong
- ▶ also the unexpected
- ▶ *forces of nature*: tsunamis, fire, biohazard, flood, polar bears, etc.
- ▶ *bad things happening*: nuclear accidents, panic, power outage, traffic, etc.
- ▶ providing safety is hard

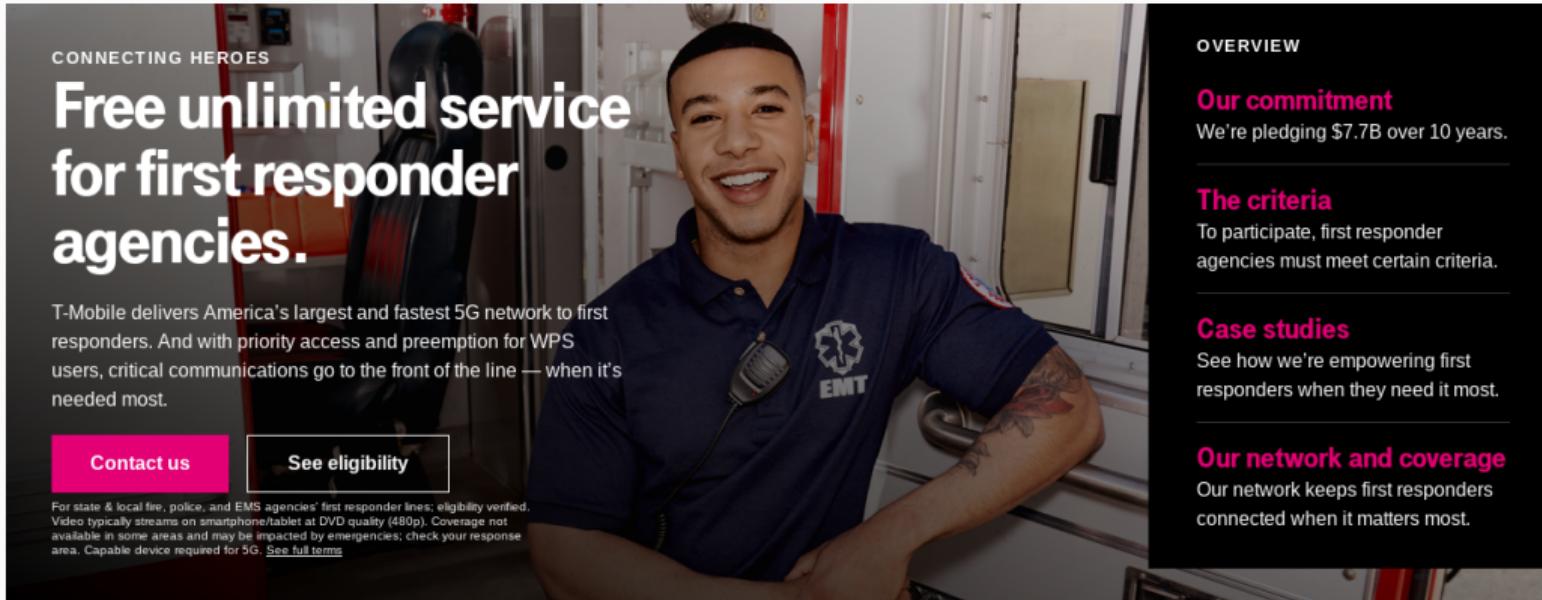


Why do we repeat this?

**Because secure networks
enable safety!**

Protecting Public Safety

How do networks protect public safety?



CONNECTING HEROES

Free unlimited service for first responder agencies.

T-Mobile delivers America's largest and fastest 5G network to first responders. And with priority access and preemption for WPS users, critical communications go to the front of the line — when it's needed most.

[Contact us](#) [See eligibility](#)

For state & local fire, police, and EMS agencies' first responder lines; eligibility verified. Video typically streams on smartphone/tablet at DVD quality (480p). Coverage not available in some areas and may be impacted by emergencies; check your response area. Capable device required for 5G. [See full terms](#)

OVERVIEW

Our commitment
We're pledging \$7.7B over 10 years.

The criteria
To participate, first responder agencies must meet certain criteria.

Case studies
See how we're empowering first responders when they need it most.

Our network and coverage
Our network keeps first responders connected when it matters most.

<https://www.t-mobile.com/business/government/first-responders-connecting-heroes>

How do networks protect public safety?

- ▶ Emergency communication
- ▶ Report an emergency



Law enforcement

- ▶ Monitor communications
- ▶ Localize individuals
- ▶ User registration



Security: against malicious activities by people

- ▶ anticipate war, terrorism, fraud, theft, abuse, etc.
- ▶ also the unexpected
- ▶ providing security is harder!
- ▶ ... because the harm is *intentional*



IT makes eavesdropping easier

- ▶ Hackers can exploit protocol weaknesses to get cleartext

ReVoLTE Attack Allows Hackers to Listen in on Mobile Calls

Author:
Elizabeth Montalbano
August 13, 2020
/ 9:06 am
2:30 minute read
 Write a comment
Share this article:
[f](#) [t](#) [...](#)



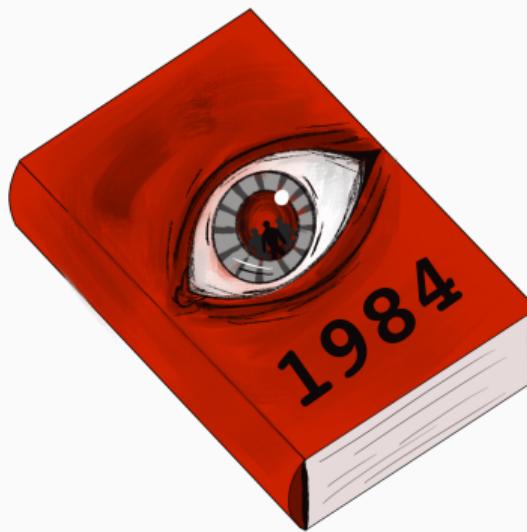
Rare attack on cellular protocol exploits an encryption-implementation flaw at base stations to record voice calls.

- ▶ Numerous other examples: WIFI's WPA2, TLS, ...

Systematic eavesdropping on all: mass surveillance

By organizations that claim to be legitimate:

- ▶ for profit: Google, Facebook, device vendors, etc.
- ▶ for *law enforcement*: governments
- ▶ using smartphone, TV, *smart speakers* ...



How did it get so bad?

On the Internet, nobody knows you're a dog.



©The New Yorker Collection 1993 Peter Steiner
From cartoonbank.com. All rights reserved.

- ▶ **1994:** SSL 1.0¹
- ▶ **1995:** SSL 2.0
- ▶ **1996:** SSL 3.0
- ▶ ...
- ▶ **1998:** Traffic Analysis of SSL Encrypted Web Browsing²

It didn't take long until encryption could be circumvented!

¹Secure Socket Layer, deprecated predecessor of TLS: Provides encryption for network connections.

²Heyning Cheng & Ron Avnur

What happened since then?



2014 "You could read anyone's email. Any website:

You can watch traffic to and from it." (Edward Snowden)

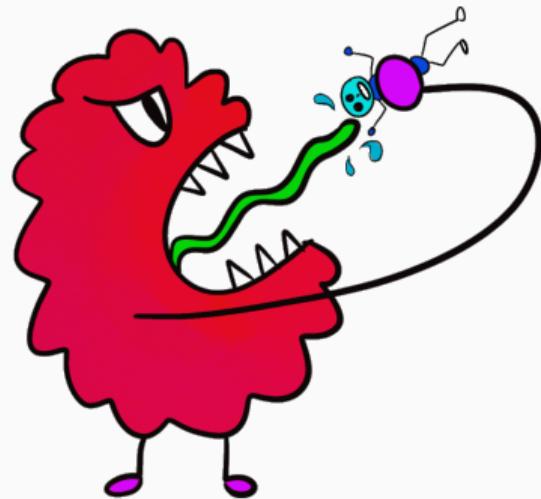
2016 Biggest data breach in history, likely by "a state-sponsored actor,"

revealing information of 500 million users.

2018 Google is probably tracking your location, even if you turn it off, says report.

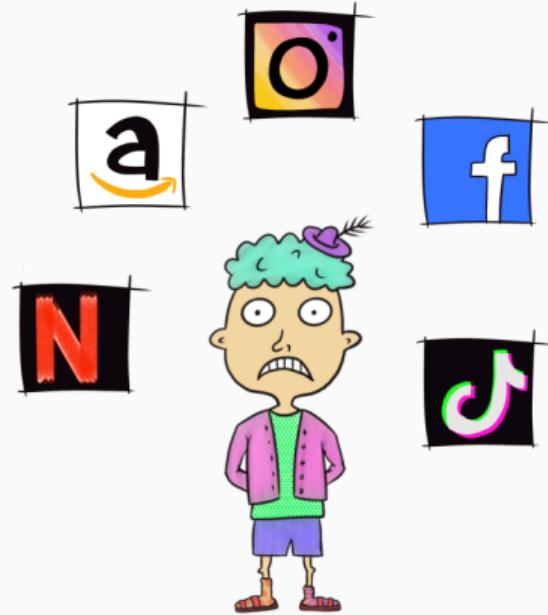
While your location history is paused, some services still store your location data.

So... Who are the bad guys here?



Official Bad Guys

- ▶ Companies with bad security
- ▶ NSA, intelligence services

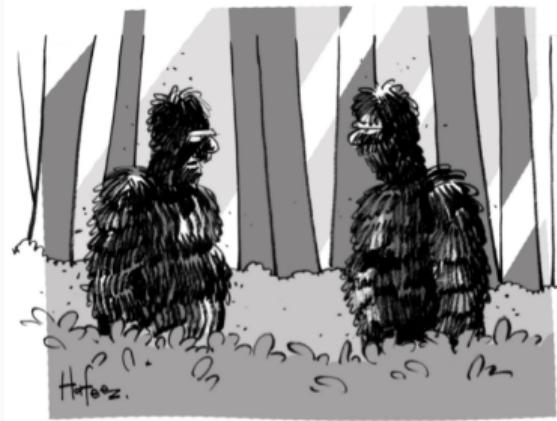


Unofficial Bad Guys

- ▶ Order all the stuff!
- ▶ Stream all the series!



O.K., go ahead
I'm on a private network.

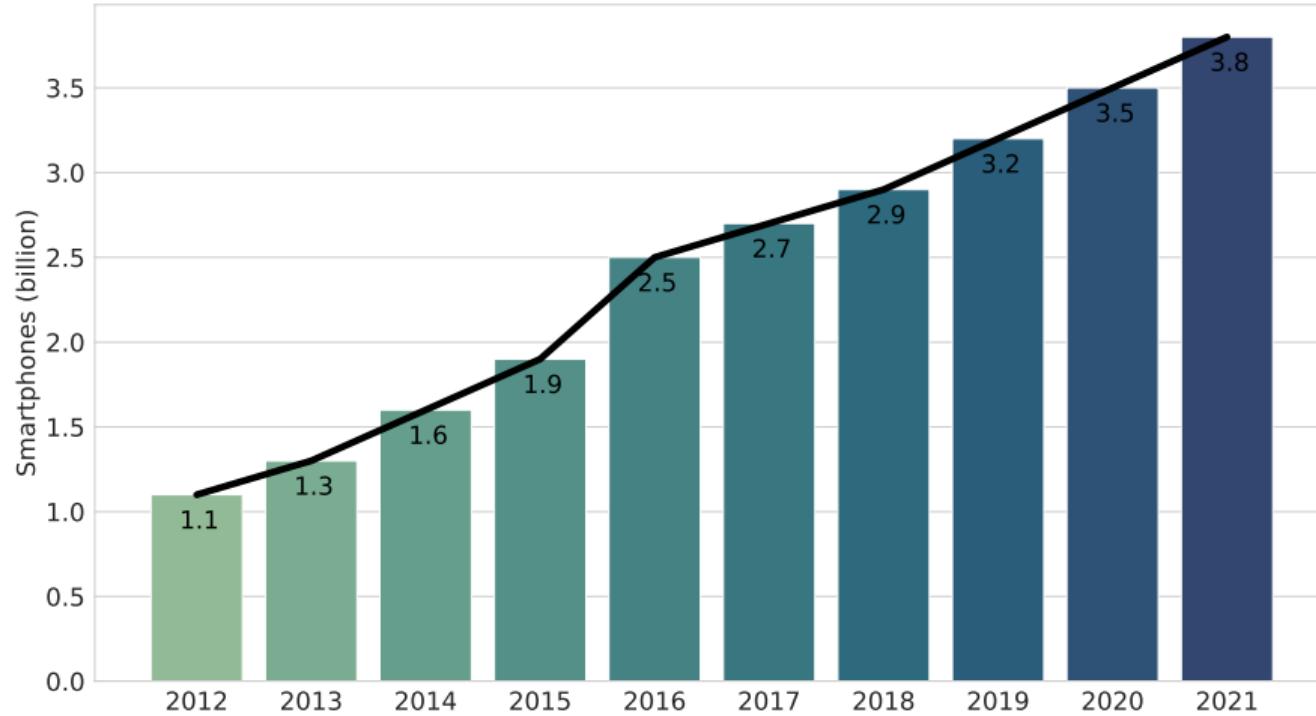


I do all my browsing on Tor.

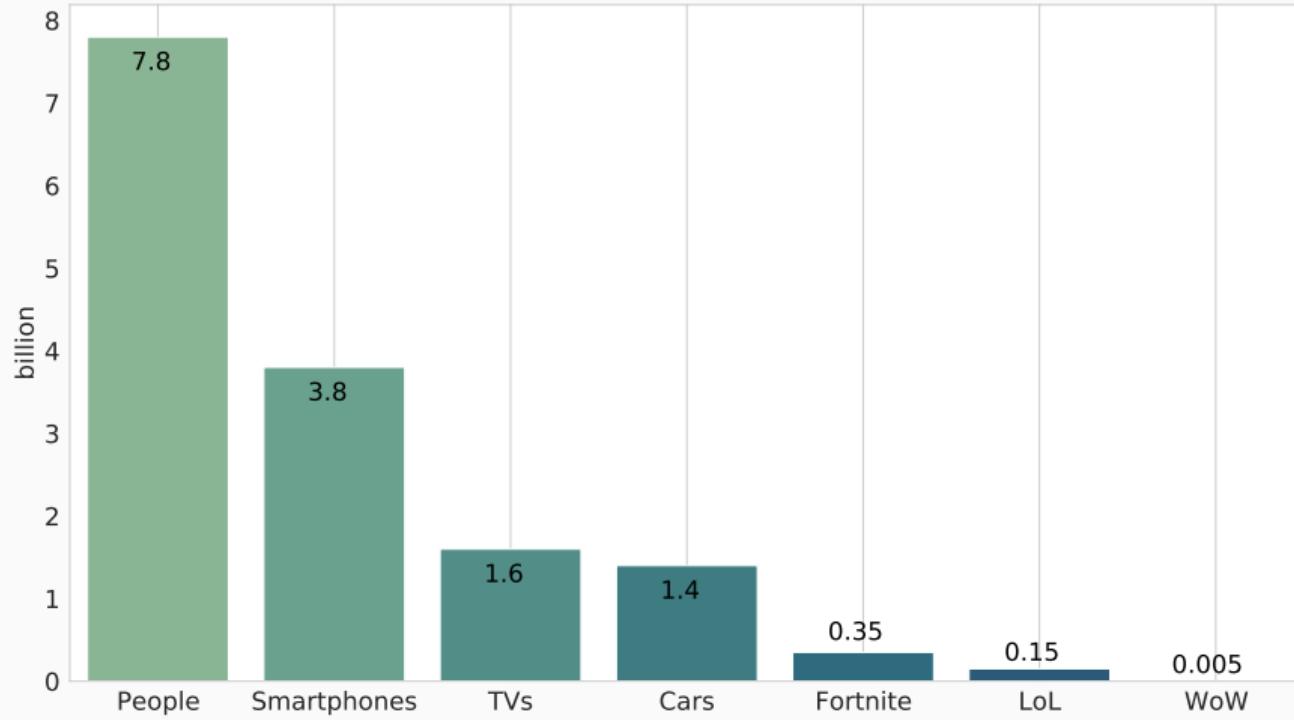
Kaamran Hafeez, 2018, The New Yorker

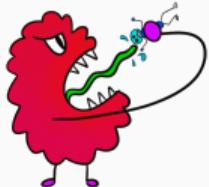
Mobile Network Security

Why Mobile Network Security?

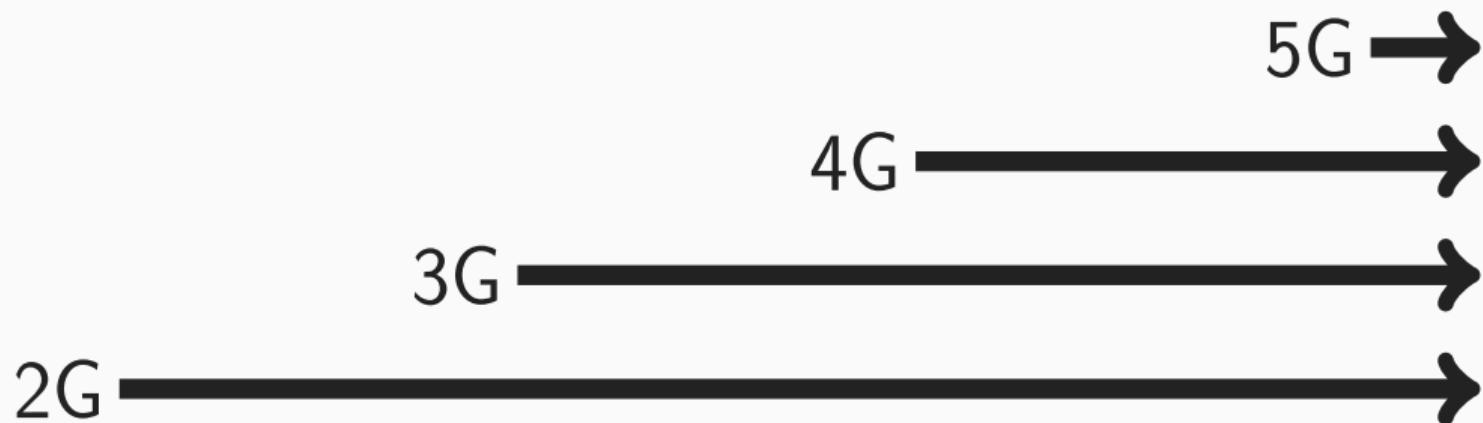


How much is that?





- ▶ Mobile networks have a complex specification
- ▶ In comparison to the Internet, they are relatively young
- ▶ Wireless connections are more problematic
- ▶ Flaw in the specification?
Affects 3.8 billion mobile users!



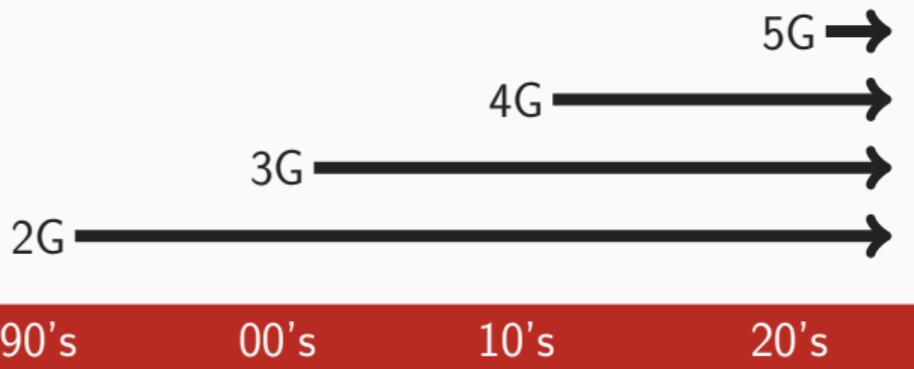
90's

00's

10's

20's

- ▶ 2G is completely broken
- ▶ 3G has many known vulnerabilities
- ▶ 4G improved but still ...
- ▶ 5G is highly similar to 4G



The image shows a screenshot of a news article from the ACLU website. The background of the article features a photograph of a mosque minaret and palm trees under a blue sky. The main title of the article is "NSO GROUP SPYWARE USED AGAINST MOROCCAN JOURNALIST DAYS AFTER COMPANY PLEDGED TO RESPECT HUMAN RIGHTS". Below the title, the date "June 22, 2020" is visible. The ACLU logo is at the top right of the page. To the right of the article, there is a sidebar with the text "NEWS & COMMENTARY" and a sub-headline: "ICE Records Confirm that Immigration Enforcement Agencies are Using Invasive Cell Phone Surveillance Devices". At the bottom of the sidebar, it says "Over a thousand pages of records begin to explain how". On the far right, there is a close-up photograph of a piece of electronic equipment with various knobs, buttons, and labels like "ANT 1", "ANT 2", "INTERNAL CONTROLLER", and "USB".

NSO GROUP SPYWARE USED AGAINST MOROCCAN JOURNALIST DAYS AFTER COMPANY PLEDGED TO RESPECT HUMAN RIGHTS

June 22, 2020

ACLU 100 YEARS

About Issues Our work News Take action

NEWS & COMMENTARY

ICE Records Confirm that Immigration Enforcement Agencies are Using Invasive Cell Phone Surveillance Devices

Over a thousand pages of records begin to explain how

ANT 1 ANT 2 INTERNAL CONTROLLER USB

There are different types of attacks:

- ▶ Realistic: Real-world incidents
- ▶ Scientific: Controlled setting, artificial scope
- ▶ Borderline: Feasible but with many limitations/requirements

In the first part of the course:

- ▶ Required background on 4G and 5G
- ▶ Attacks:
 - DNS Redirection, Website Fingerprinting, Identification
 - Decrypting calls
 - SUCI Catcher

Internet and Web Security



This is the second part of the course.