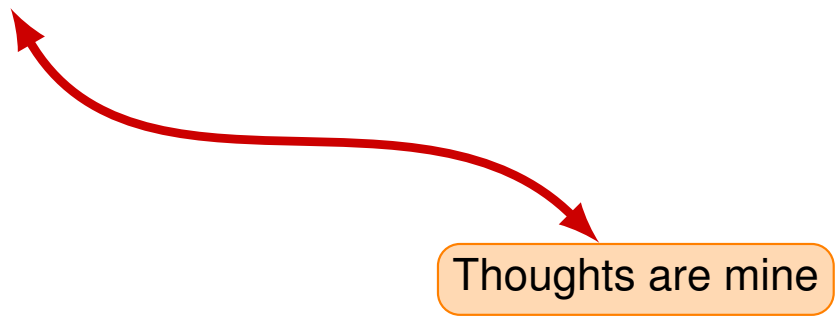
SwissCovid Status

Serge Vaudenay

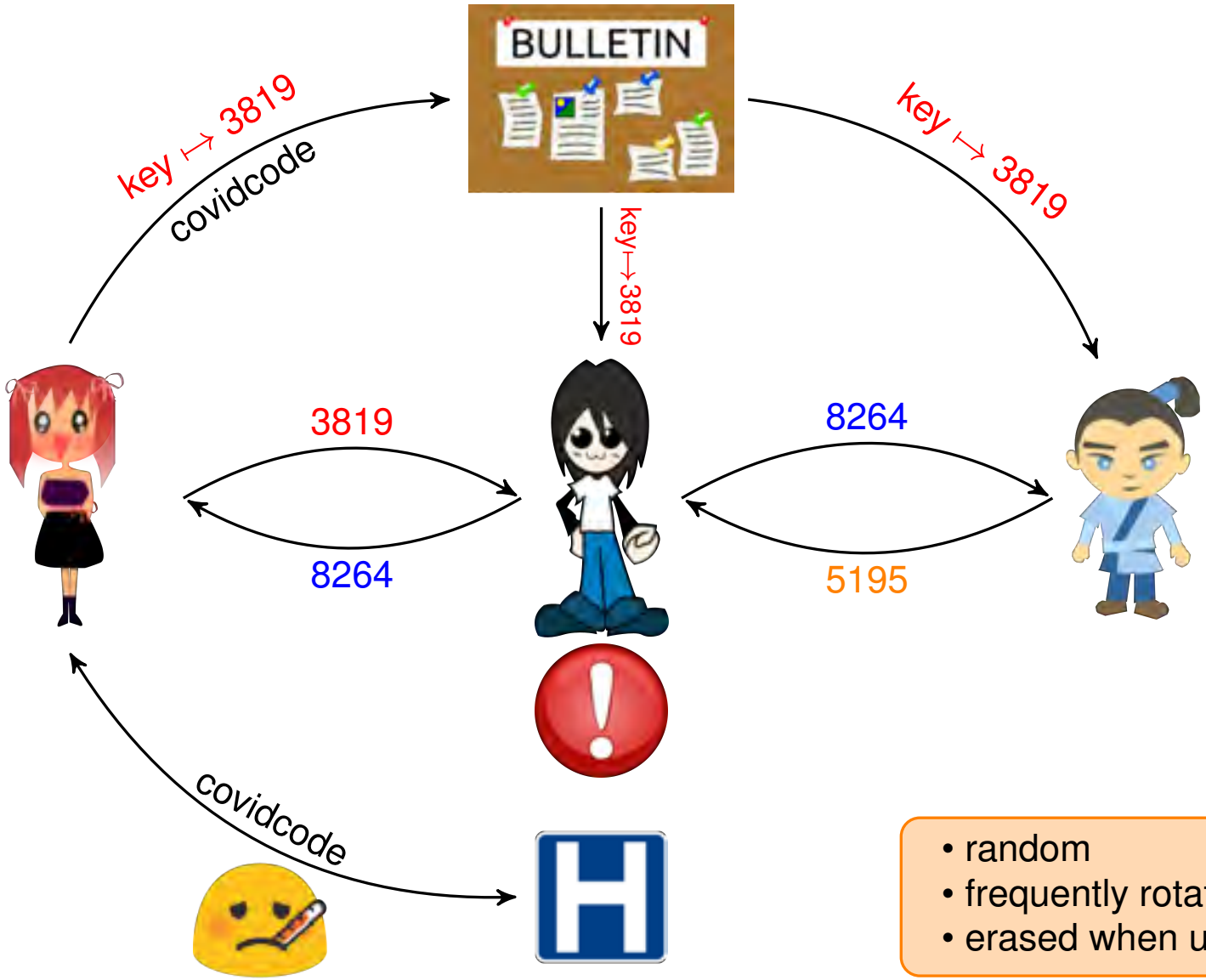
EPFL



EPFL Giving SwissCovid to Humanity

[Prometheus]

Decentralized Contact Tracing

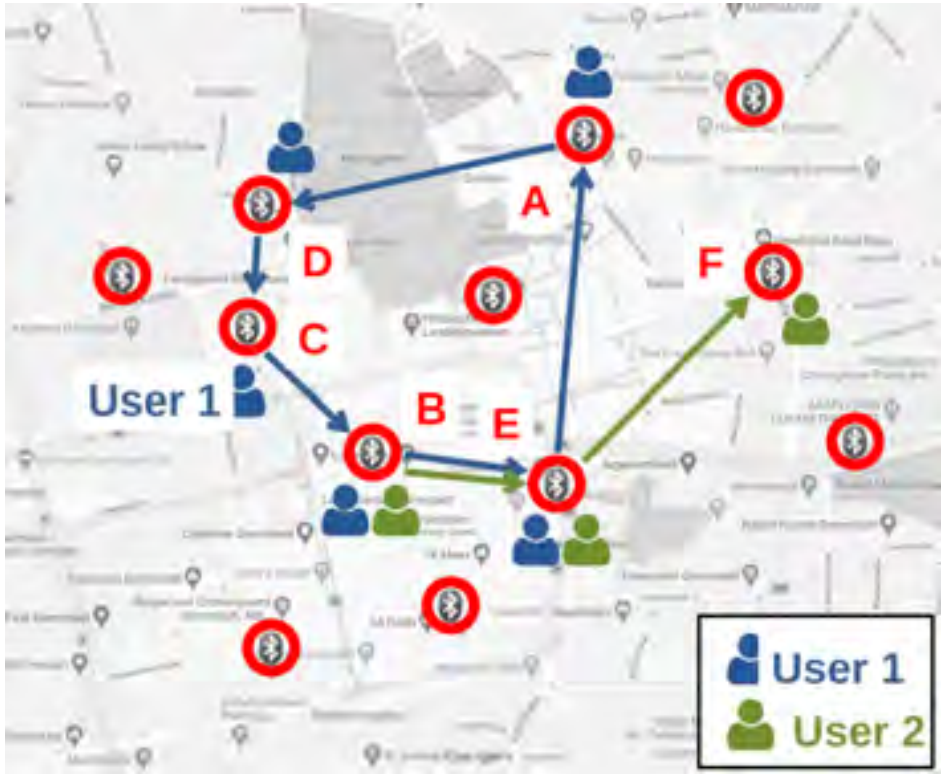


- random
- frequently rotated
- erased when useless

DP-3T

Decentralized Privacy-Preserving Proximity Tracing

- users can be tracked by sniffing Bluetooth
- reporting users can be identified and tracked



Mind the GAP: Security & Privacy Risks of Contact Tracing Apps

`https://arxiv.org/abs/2006.05914`

DP-3T Making a Pact with Apple/Google

[Faust]

Legal Basis vs GAEN

LEp Art.60a (June 20)

Law on epidemics

- al.5e: source code must be public for all components
- al.7: government is in charge of details

$\rightarrow$ OSTP (June 24)

Ordinance on the proximity tracing system for coronavirus

- Art.2: components are ... [not GAEN]
- Art.5 al.2: tasks of SwissCovid *with the help of an interface of the operating system*
  - daily key generation
  - exchange over Bluetooth
  - storage of received keys
  - download of keys and comparison
  - notification
- Art.5 al.3: the *functions of the operating system* do not need a public source code

Legal Basis vs Bluetooth Reliability (Space)

OSTP (June 24) Art.5 al.2e:

notify proximity (up to 1.5m) to a reported user

- Leith-Farrell 26.6.2020:
  Measurement-Based Evaluation Of Google/Apple Exposure Notification API For Proximity Detection In A Light-Rail Tram
  $\rightarrow$ testing $d < 1.5$m not better than random
  `https://journals.plos.org/plosone/article?id=10.1371/journal.pone.0239943`
- Params have been increased (twice) to more sensitivity
  $\rightarrow$ In lab experiment conditions:
  $\Pr[\text{spot}|d = 1.5\text{m}] = 57.3\%$, $\Pr[\text{spot}|d = 3\text{m}] = 45.6\%$
  `https://github.com/admin-ch/PT-System-Documents/blob/master/SwissCovid-ExposureScore.pdf`

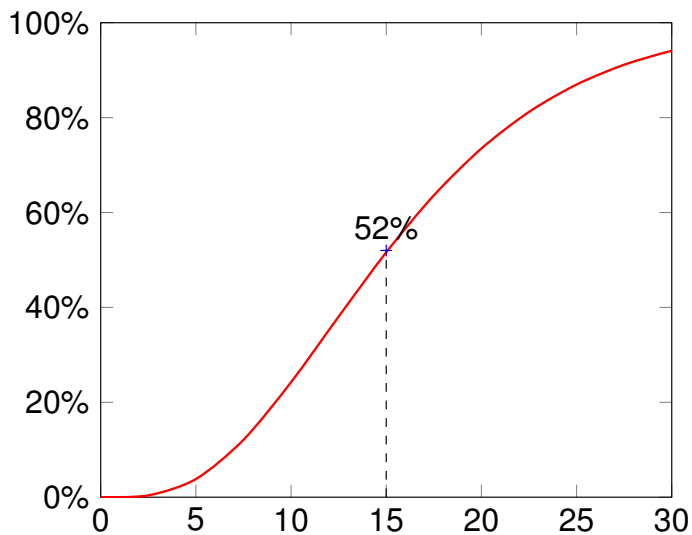
Legal Basis vs Bluetooth Reliability (Time)

OSTP (June 24) Art.5 al.2e:

notify proximity (for at least 15min) to a reported user

- GAEN scans Bluetooth once every 4min
- During an event of duration $T \to +\infty$ with a total proximity of $\lambda \times$ 4min, the probability to have k scans is $\frac{\lambda^k e^{-\lambda}}{k!}$

$$\Pr[\text{spot}|\lambda \times 4\text{min}] \approx 1 - \left(1 + \lambda + \frac{\lambda^2}{2!} + \frac{\lambda^3}{3!}\right) e^{-\lambda}$$



[Back to the Future: *Never set it to 2020*]

Eprint 2020/1393

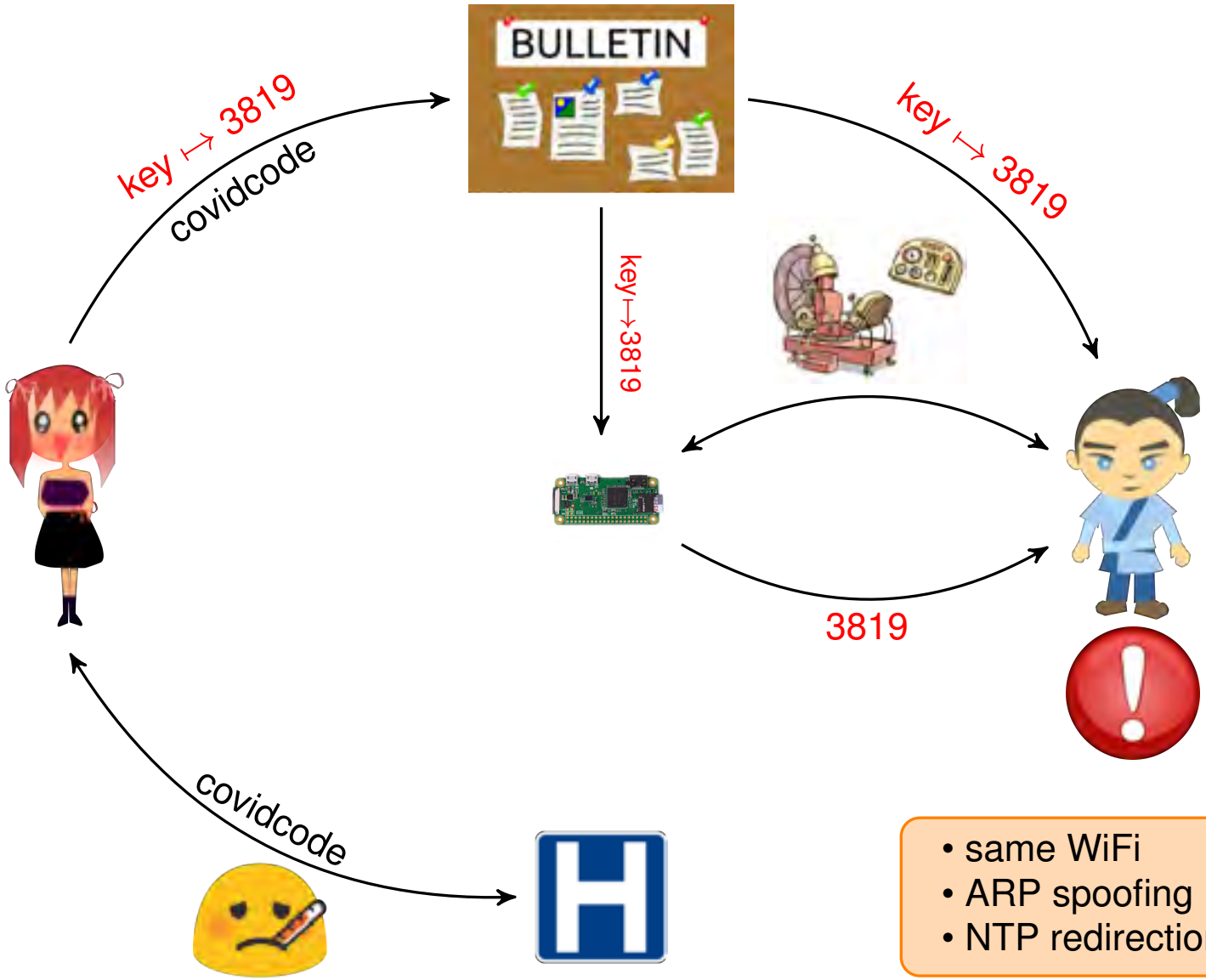
On the Effectiveness of Time Travel to Inject COVID-19 Alerts*

Vincenzo Iovino[1], Serge Vaudenay[2], and Martin Vuagnoux[3]

[1] University of Salerno, Italy
[2] EPFL, Lausanne, Switzerland
[3] base23, Geneva, Switzerland

Abstract. Digital contact tracing apps allow to alert people who have been in contact with people who may be contagious. The Apple/Google Exposure Notification (EN) system is based on Bluetooth proximity estimation. It has been adopted by many countries around the world. However, many possible attacks are known. The goal of some of them is to inject a false alert on someone else's phone. This way, an adversary can eliminate a competitor in a sport event or a business in general. Political parties can also prevent people from voting.
In this report, we review several methods to inject false alerts. One of them requires to corrupt the clock of the smartphone of the victim. For that, we build a time-traveling machine to be able to remotely set up the clock on a smartphone and experiment our attack. We show how easy this can be done. We successfully tested several smartphones with either the Swiss or the Italian app (SwissCovid or Immuni). We confirms is also works on other EN-based apps: NHS COVID-19 (in England and Wales), Corona-Warn-App (in Germany), and Coronalert (Belgium).

Time Travel can make False Alert Injection



- same WiFi
- ARP spoofing
- NTP redirection

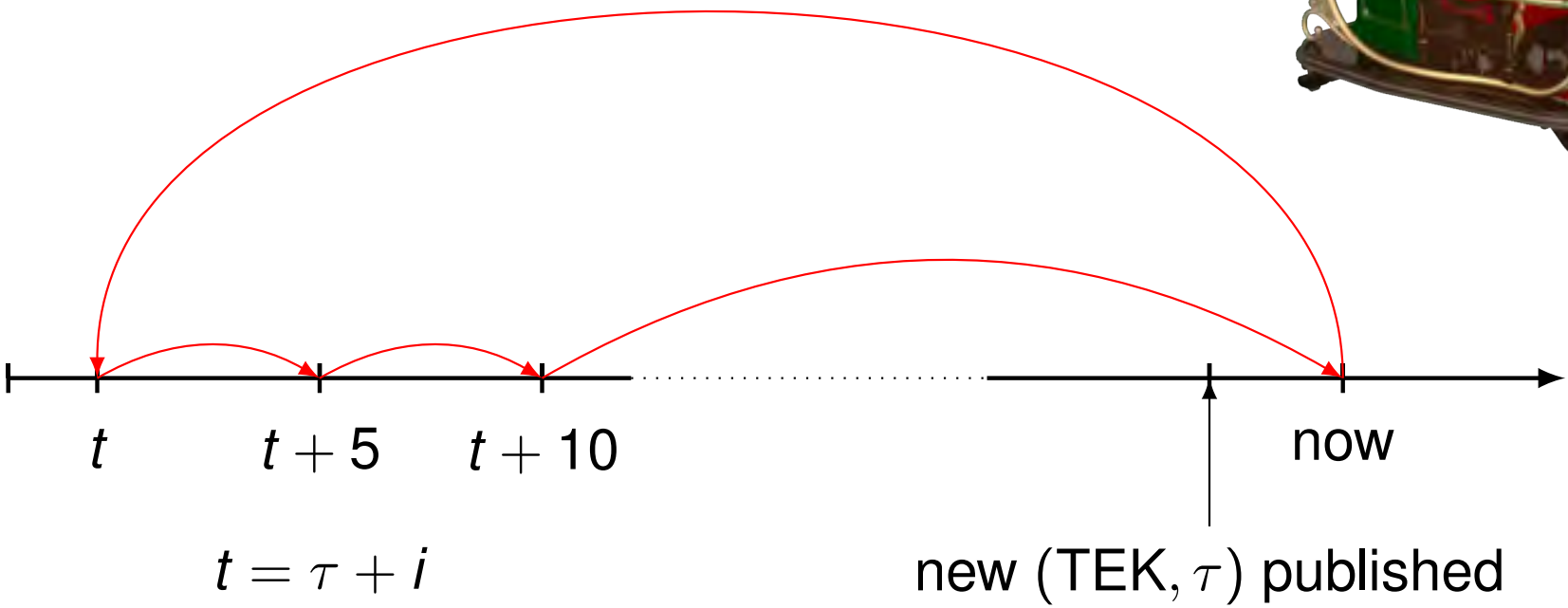
Ways to Build a Time Machine

- set clock by physical access / intrusion
- rogue NTP server

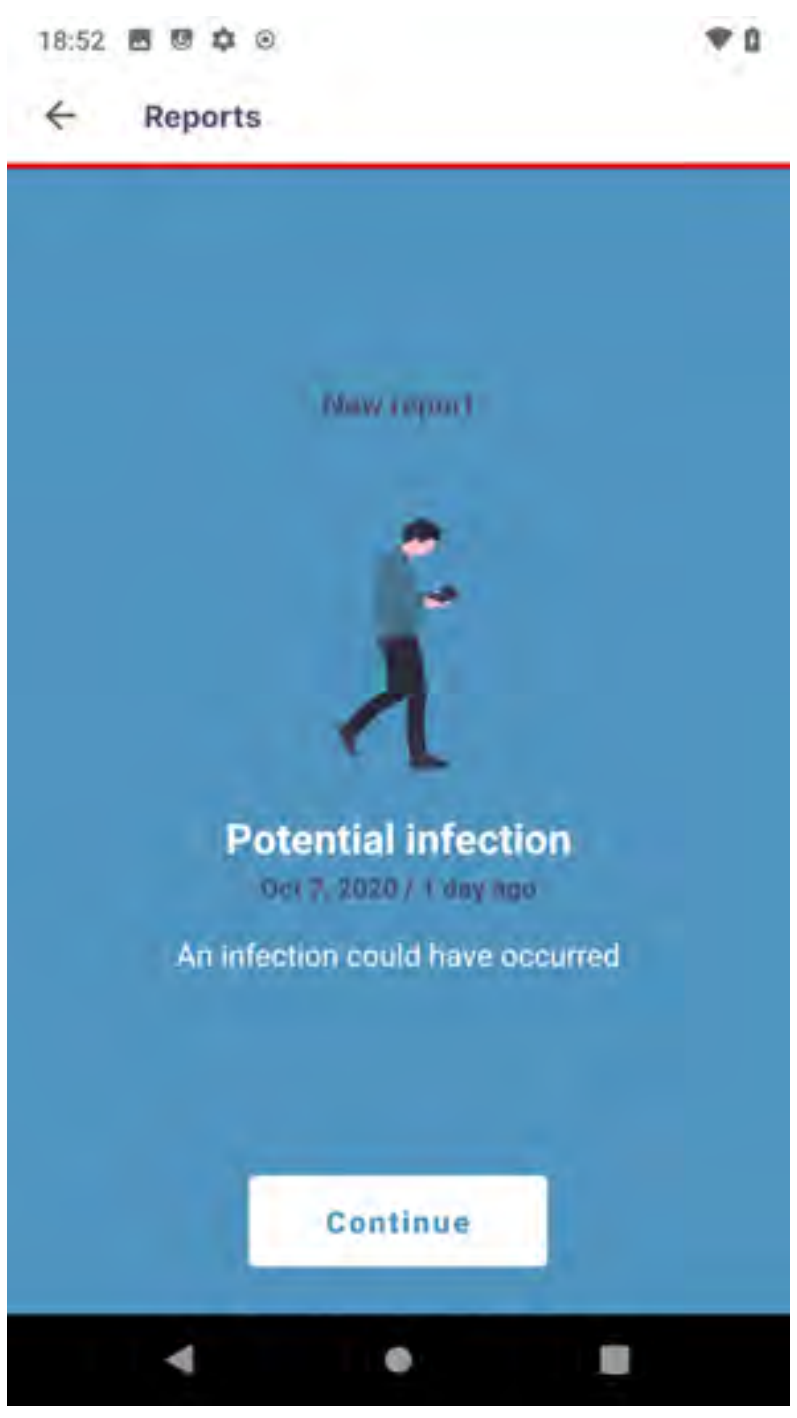
- rogue base station

- rogue GNSS

Multiple Time Jump Attack

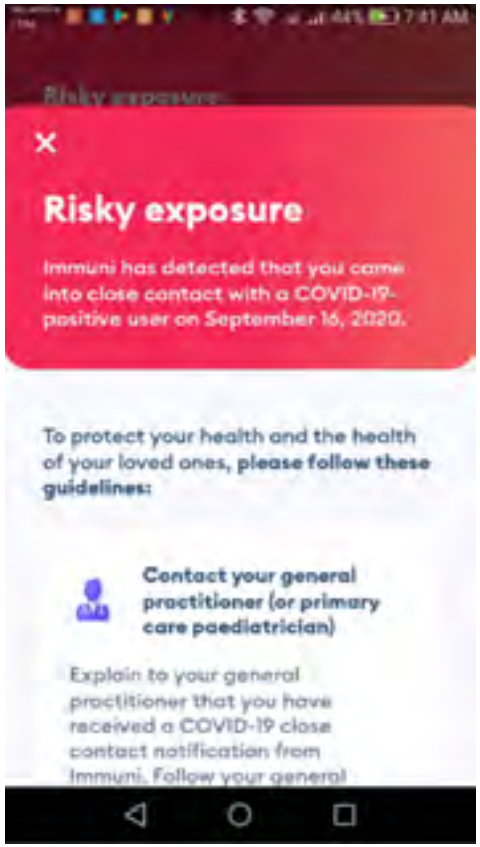


total duration: 1 second...
could easily be done massively over a radius of 500m

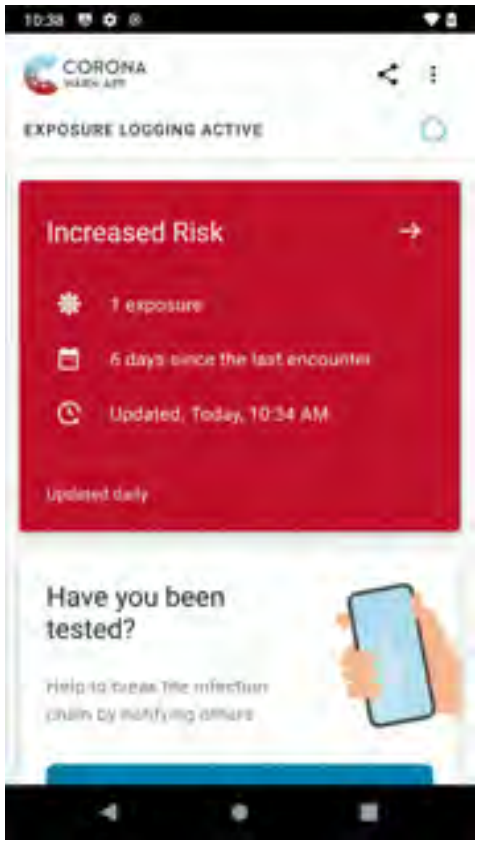

18:52
Reports
New report
Potential infection
Oct 7, 2020 / 1 day ago
An infection could have occurred
Continue

More Apps

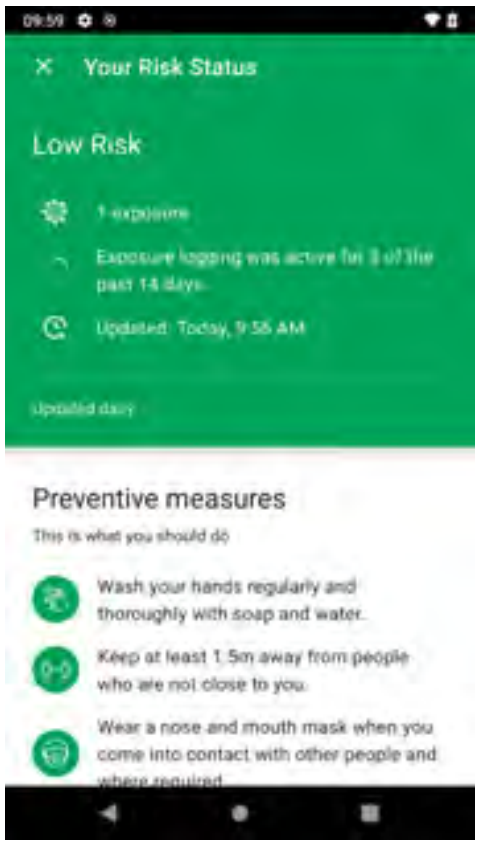
Immuni (Italy)



Corona-Warn (Germany)

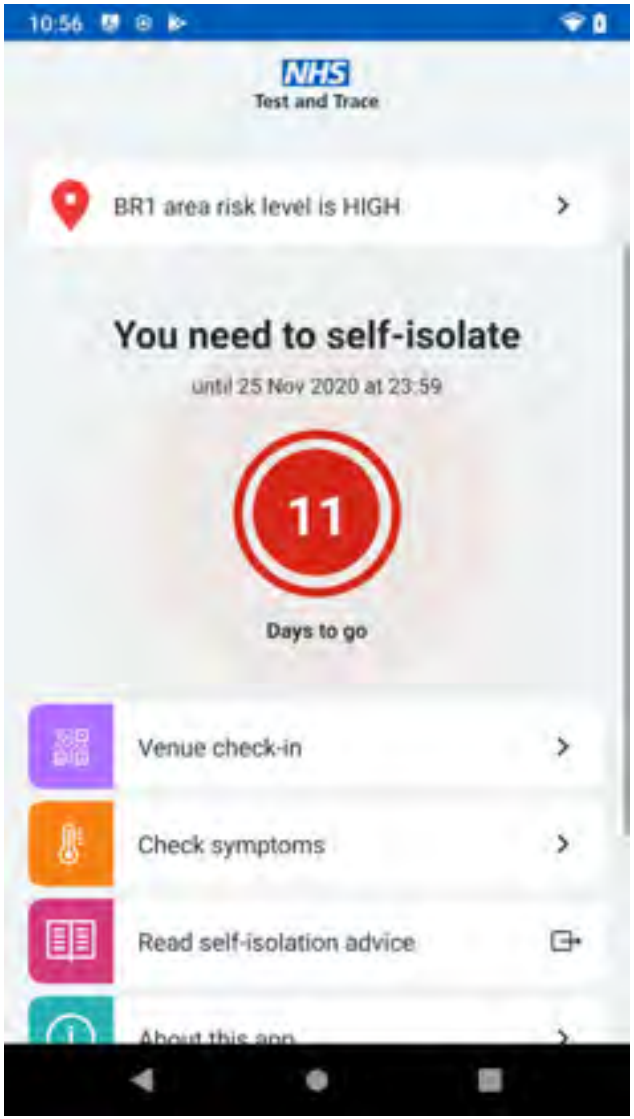


Coronalert (Belgium)

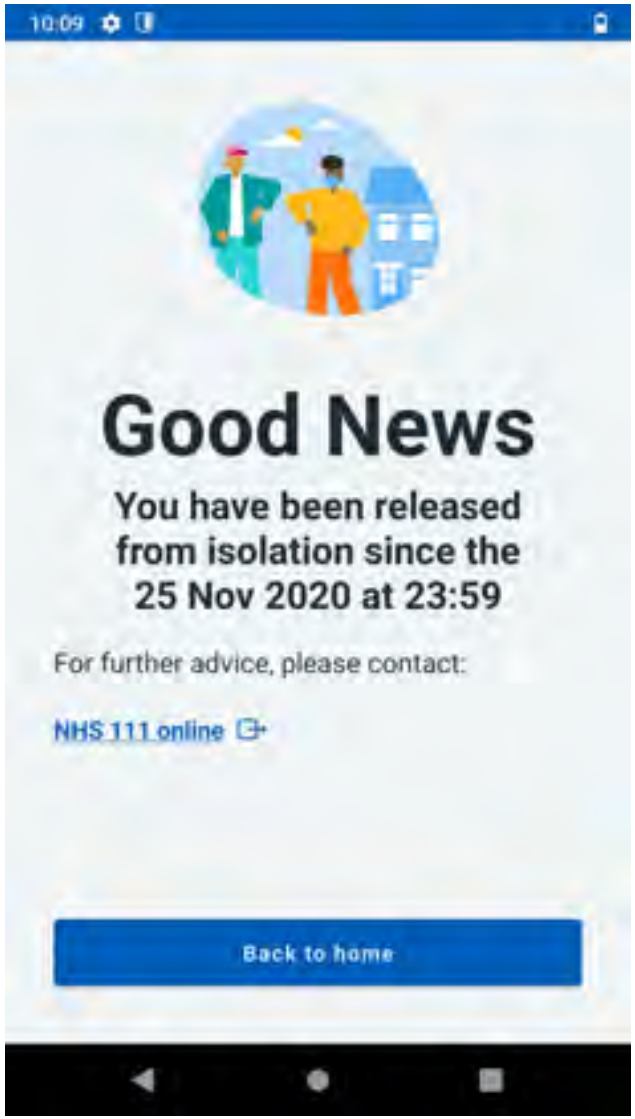


NHS COVID-19 (England and Wales)

Alert



Good news



An Act of Faith

“we should trust SwissCovid”

[Disney illustration]

Adoption

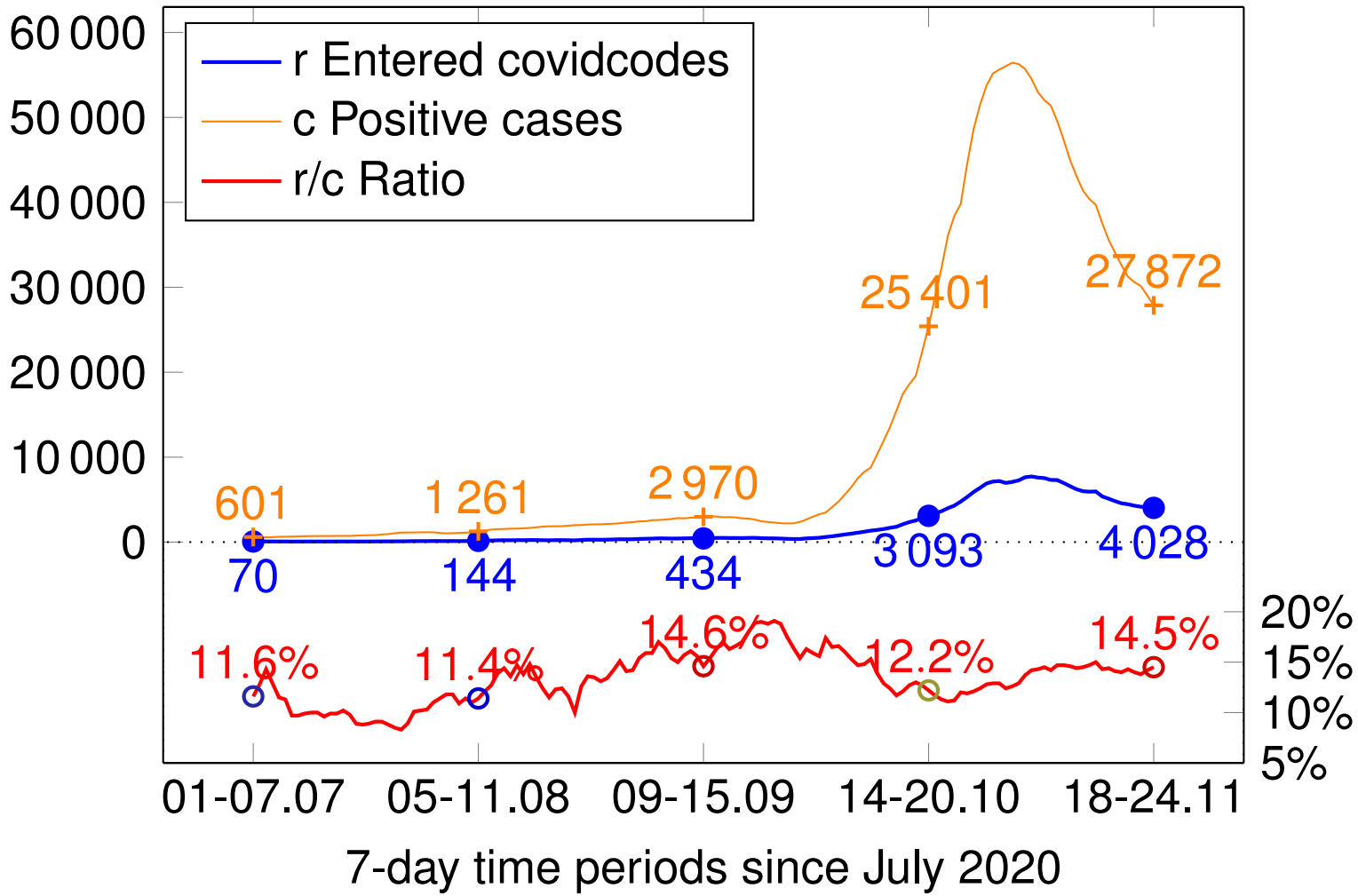
used by 22% of population (tricky to count activations)

Reasons for not using:

- "**37%: perceived lack of usefulness of the app**"
  - only useful if we stay close to strangers for a long time
- "**23%: not having a suitable smartphone or OS**"
  - must have a smartphone with iOS or Android
  - must not be too old
  - must not be Chinese and too recent
  - must not be deGoogled
- "**22%: concerns about privacy**"
- various other reasons

→ Von Wyl et al. medRxiv 2020.08.29.20184382.
`https://doi.org/10.1101/2020.08.29.20184382`

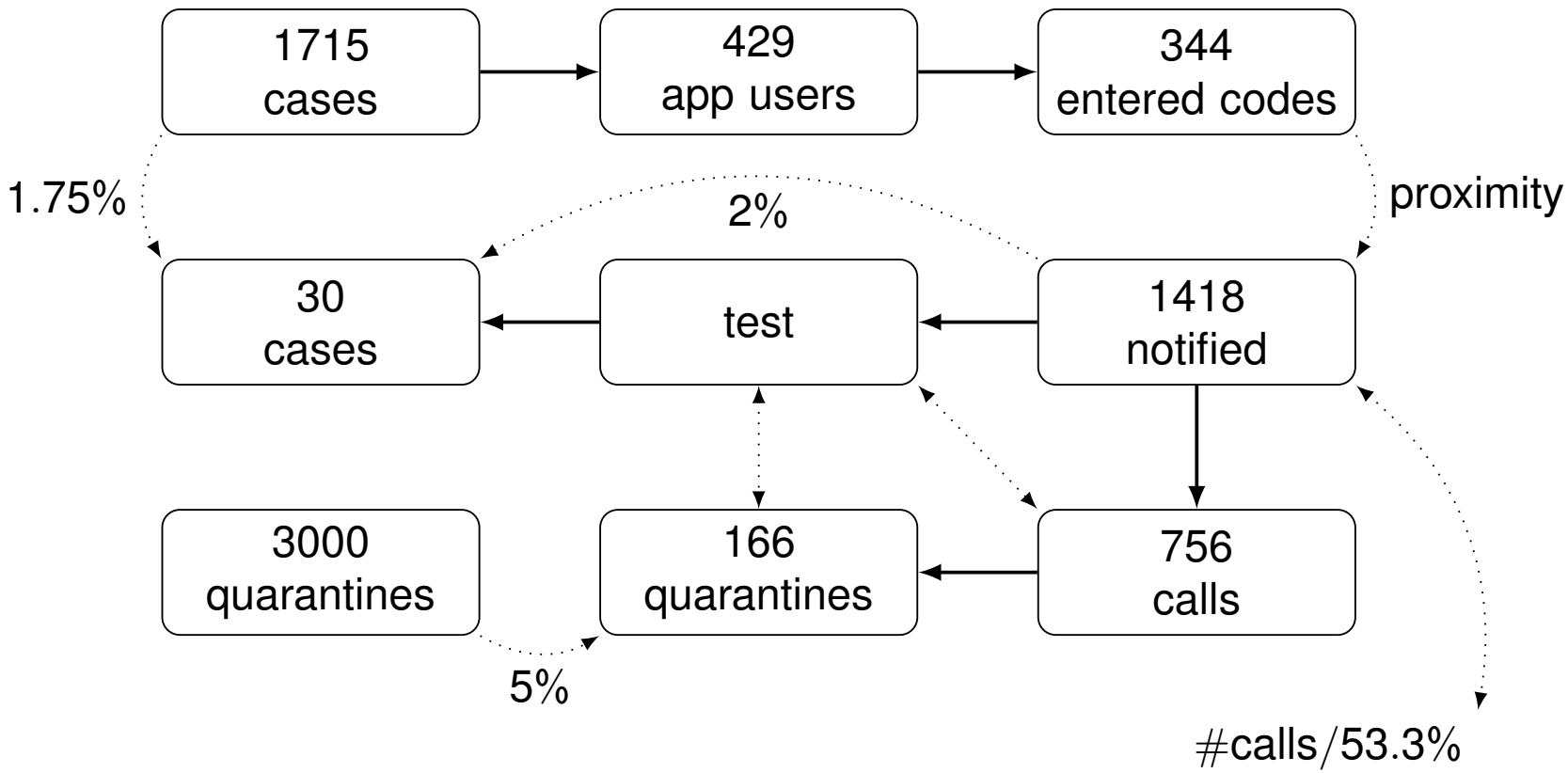
Number of Cases in SwissCovid



The Contribution of the SwissCovid [...] in ZH

Von Wyl (Work in Progress)

https://www.ebpi.uzh.ch/dam/jcr:5fc56fb7-3e7e-40bf-8df4-1852a067a625/Estimation%20of%20SwissCovid%20effectiveness%20for%20the%20Canton%20of%20Zurich%20in%20September%202020_V1.5.pdf



Alternative

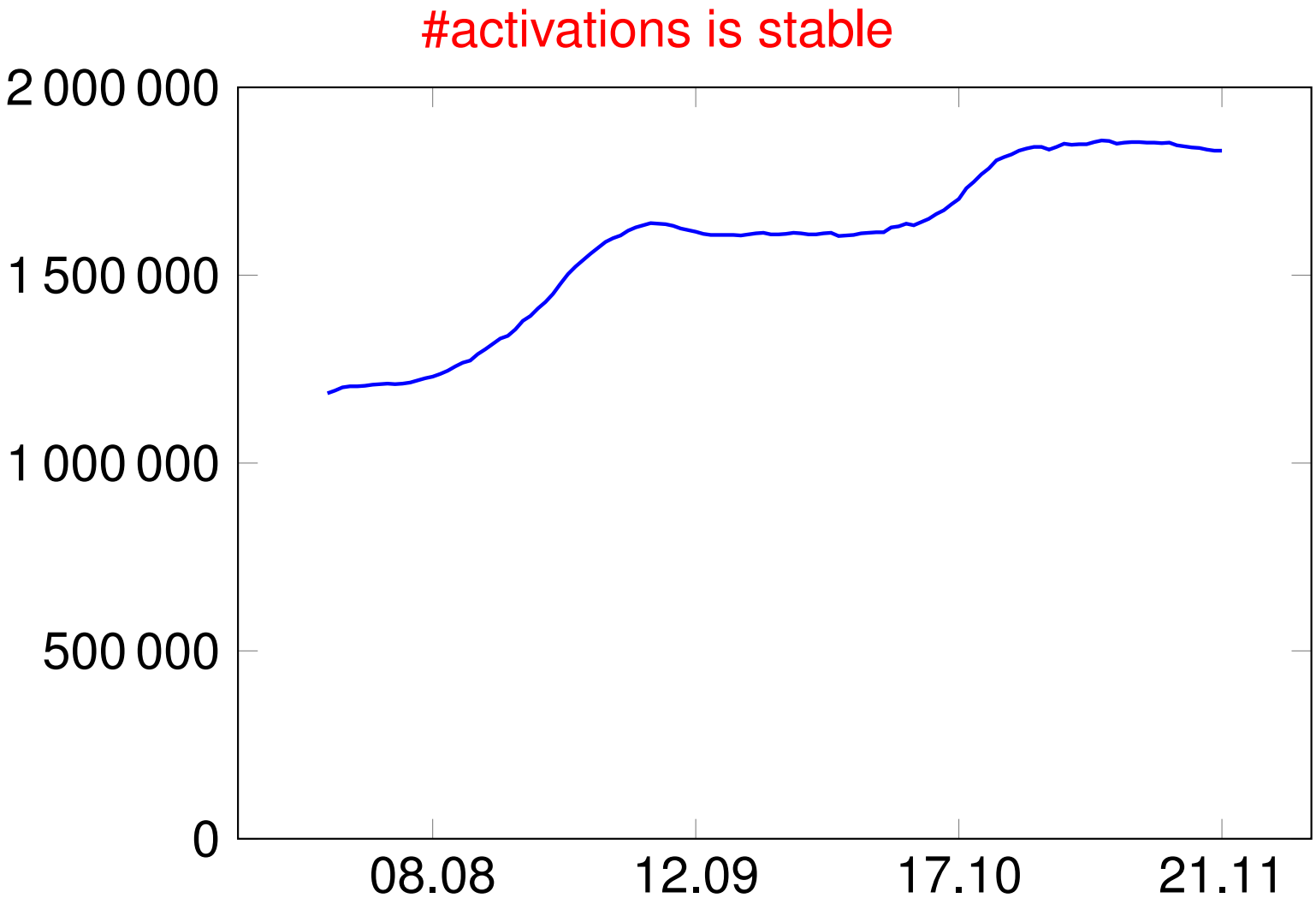
Conclusion

Much Ado About Nothing

- many broken promises
- usefulness is far from proven

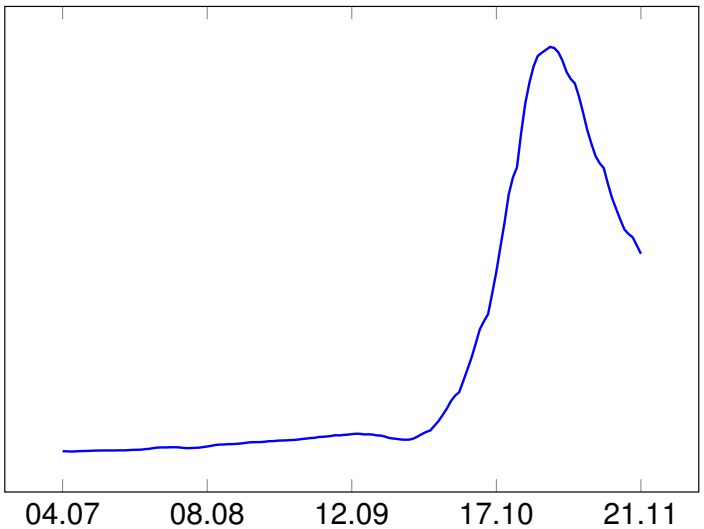
`https://lasec.epfl.ch/people/vaudenay/swisscovid.html`

Empirical Rule #1

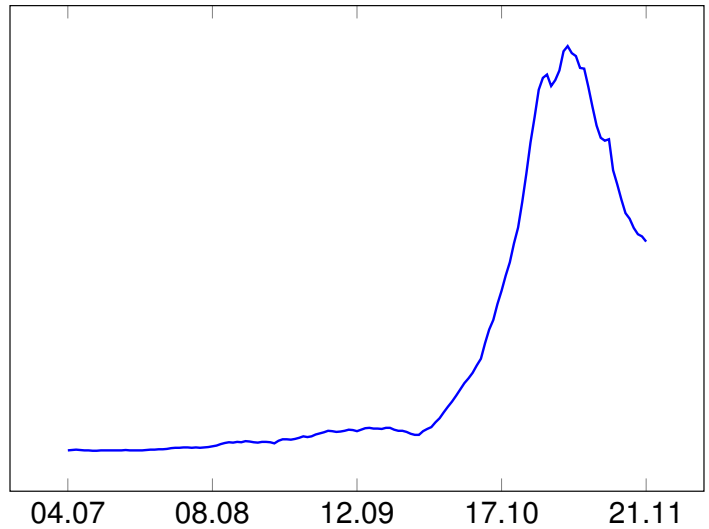


Empirical Rule #2

#cases

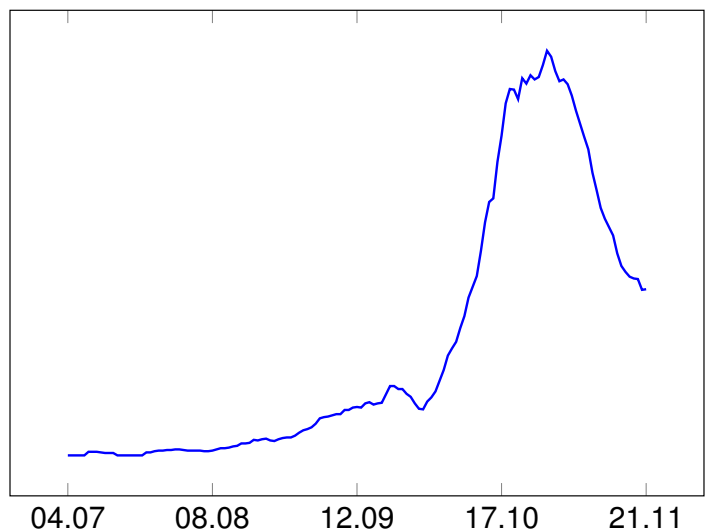


#codes



all are proportional

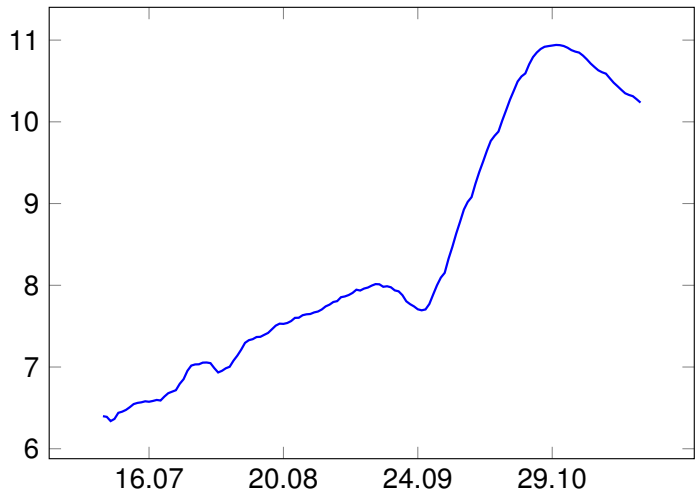
#calls



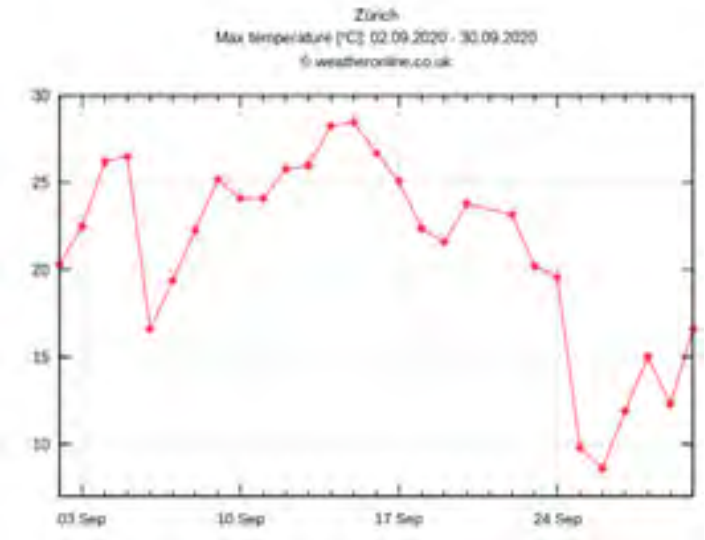
Empirical Rule #3

what happened in September?

log(#cases)

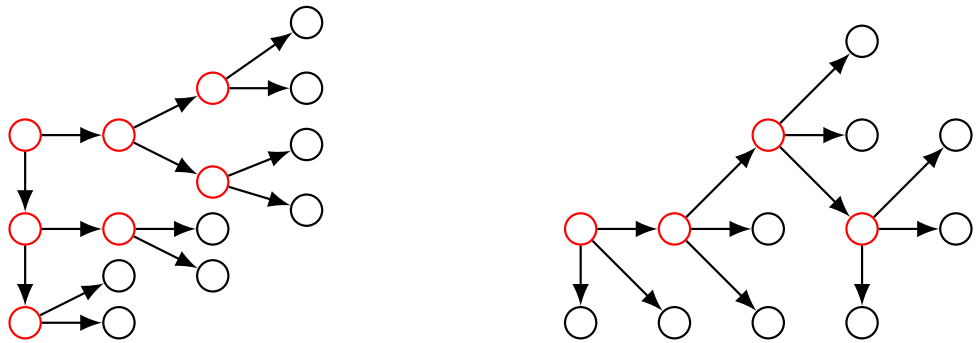


temperature in Zurich



curves jump when temperature drops

Our Naïve Contact Tracing



- 19% of cases are responsible of 80% of transmissions
  $\rightarrow$ Dillon C. Adam at al. Nature Medecine 2020.

  `https://doi.org/10.1038/s41591-020-1092-0`
- Digital contact tracing should rather be done backward
  $\rightarrow$ Sadamori Kojaku et al. arXiv (May 5!) 2020.

  `https://arxiv.org/abs/2005.02362`

OSTP (June 24) Art.6:
keys to report start two days before the first symptoms