TOPIC: 6.857 Applied Cryptography & Security

DATE: 4/11/22

FILE UNDER: L19 - Exposure Notification

PAGE: 1

Admin:

Projects - presentations start Wed 4/27 } evaluations by Wed

Quiz

Pset #4

Today:

Exposure Notification

TOPIC:

DATE: 4/11/22

FILE UNDER:

PAGE L19 2

Intro:

MCT: explain

https://youtube.com/watch?v=qQYM25pciLo
or dsf6nwxxaVo

Advantages:
- Speed
- Handle Unknown Contacts
- Works when PM Overloaded
- Privacy

Sensing

TC4TL – 6 ft. 15 min (?)

video of robots FM phantoms

orientation of phone
distance
water (bodies) in between
xmit power & model of xmitr phone
indoor/outdoor
masks?
walls
broken up exposures 3x 5min?
can hear up to 30M away?

Record: time
power (RSSI)
orientation
location

Apple/Google collaboration GAEN
Google/Apple exposure notification

TOPIC:

DATE: 4/11/22

FILE UNDER:

PAGE: L19 3

What to transmit?

- time-varying "chirp"
  (RPI - rolling proximity identifier)

  based on time & daily key
  (key mostly for compression)

  chirp = hash(key || time) (time to 15 mins)

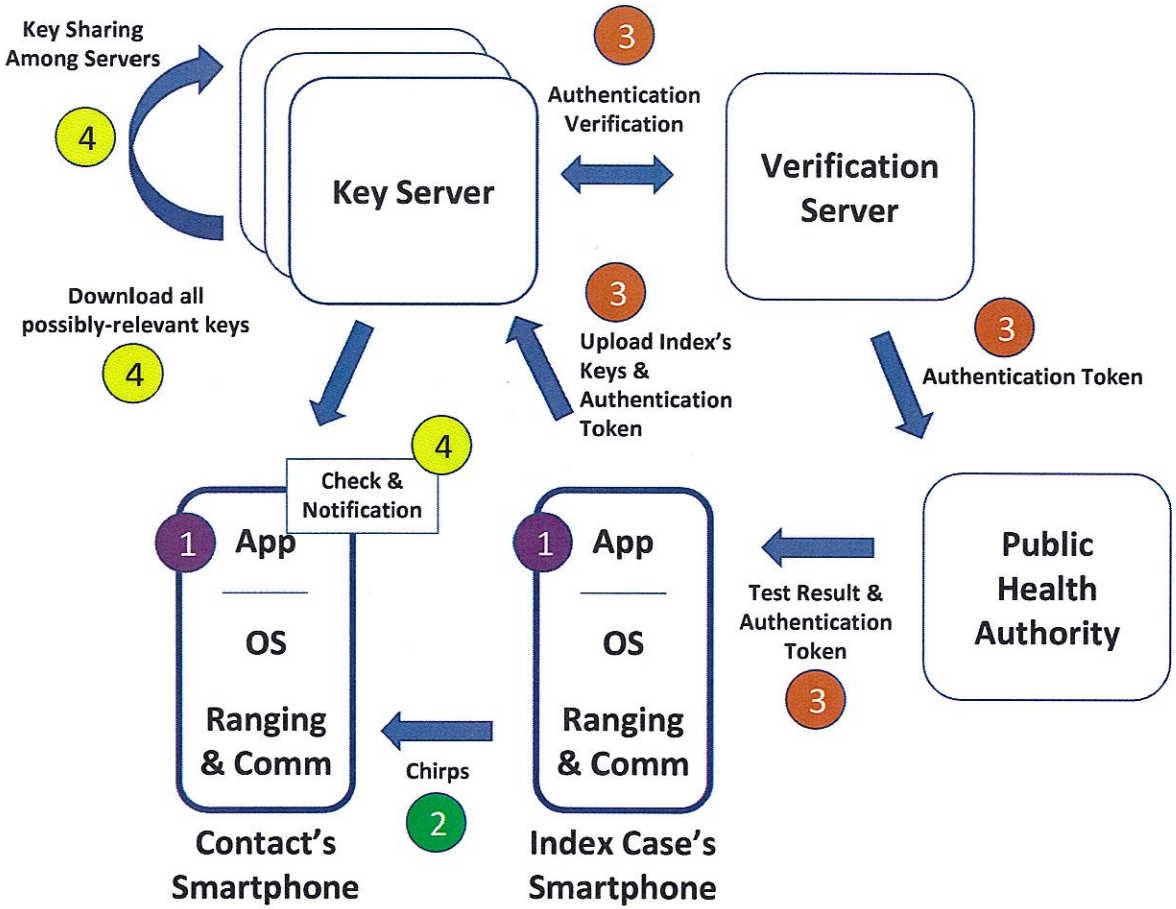
TOPIC:

DATE 4/11/22

FILE UNDER:

PAGE: L19 4

(Draw figure on board)



Steps

1. Install and enable app
2. Use keys to broadcast chirps
3. Test; if positive, upload keys
4. Download keys, check chirps heard, possibly notify of exposure

TOPIC:

DATE: 4/11/22

FILE UNDER:

PAGE: L19 5

When to upload?

When test positive!

✓ PCR tests

DIY (antigen) tests

symptoms

Authentication (Authorization)

Auth code from PHA or test administrator

to prevent spamming of DB

consent required to upload

What to upload?

test type?

day # since infected? (estimate)

TOPIC:

DATE: 4/11/22

FILE UNDER:

PAGE: L19 6

When / what to download? How to estimate risk level?

- Periodically
- use risk formula to determine risk level

  wide-net

  narrow net

- note: must re-generate chirps from keys
- can't reconstruct "social graph"
- consent needed to take action if notified

TOPIC:

DATE: 4/11/22

FILE UNDER:

PAGE: L19 7

Attacks:

- Tracking (Linking)
- Relay attacks (simultaneous)
- Replay attacks (later) (pickup RPIs from test site)
- spam DB ⇒ false notifications
- PH knows who tested positive, but not by whom

TOPIC:

DATE: 4/11/22

FILE UNDER:

PAGE: L19 8

Effectiveness:

- reduce R_0 (# infected by contact)
- scales as p^2, where p = fraction with app
- Christoph Fraser et al. estimate 600K lives saved in UK.
- PH frustrated by lack of data (due to privacy)
- may depend on advice given as to what to do if notified
- see Prof talk by HCG 4/25 Monday 4.85] guest lecture

TOPIC:

DATE: 4/11/22

FILE UNDER:

PAGE 19 9

Issues & extensions!

- fixed beacons & fixed QR codes
- record what you send, rather than what you hear
  (e.g. index uploads what he heard
- CO2 sensor?
  Indoor/outdoor sensor?
  Fitbit?
- Governance – who decides what?
  PH versus private corporations?
  LE access? (centralized schemes)
- integration with MCT?
- multiple jurisdictions?