Computer Security (COM-301)

Adversarial thinking and threat modelling

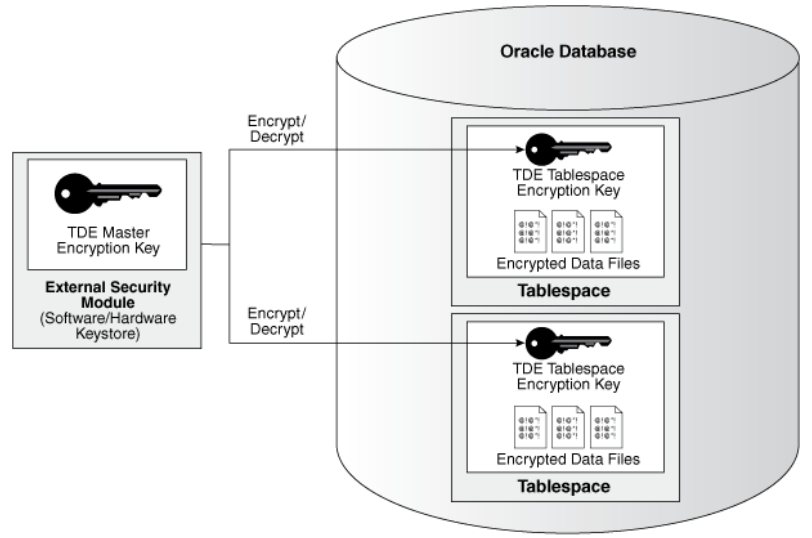
Live exercise solving

Carmela Troncoso

SPRING Lab

carmela.troncoso@epfl.ch

What can go wrong?

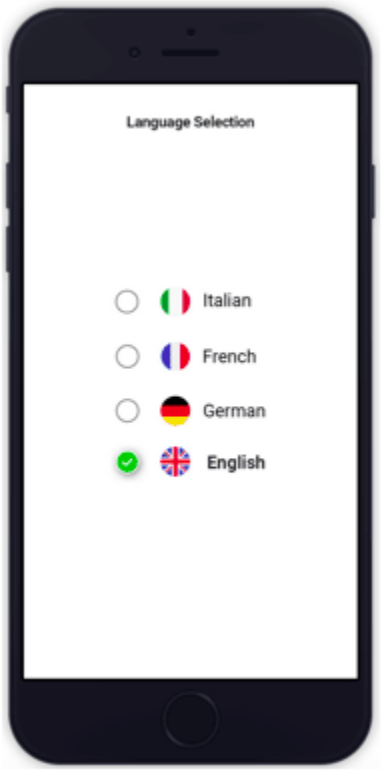


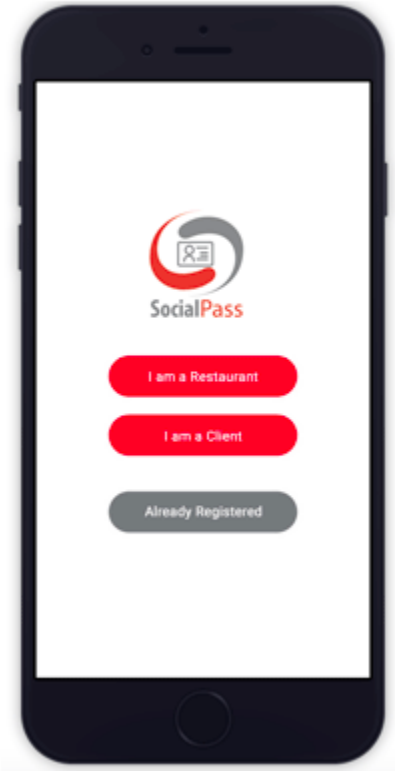
To increase the security of *data at rest* your company has introduced Transparent Data Encryption (TDE) in the databases. This way, all data in the hard drive is encrypted.

They assume that the adversary is anyone that is not an employee and does not have a login.

Propose a means for an adversary to obtain capabilities outside of this threat model

Social Pass


Language Selection
Italian
French
German
English


SocialPass
I am a Restaurant
I am a Client
Already Registered

Social Pass

Download SocialPass to your smartphone and enter the data that will allow us to contact you easily.
Your phone number is automatically checked by SMS. A **secure QR code is generated** on your phone. This is your **Pass** that will remain on your phone and that you can use in other establishments without re-entering your data.

At the entrance to a restaurant, an event or a place of any kind:
There are two possibilities, depending on the establishment and the canton.

A) **Scan the Qr Code of the establishment**. You scan the QR Code yourself at the entrance or on the table. The establishment may be able to check it.

B) **Show your Pass.** Your pass will be scanned by the restaurant, the event organiser, the sports club, etc.

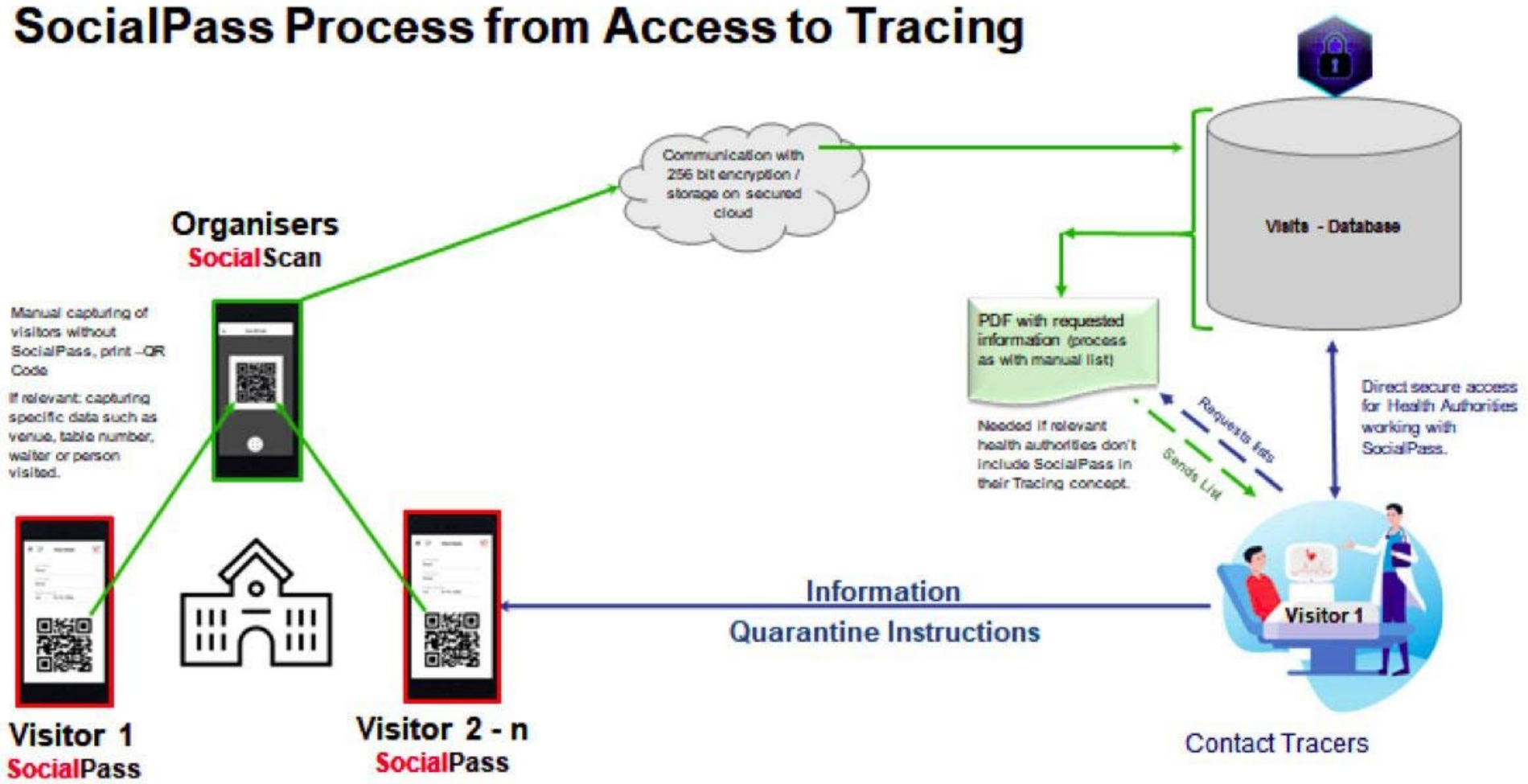
The data of your Pass will be stored directly in a secure "Swiss Cloud". **After 14 days they will be automatically deleted.**

If a person tests positive, the authorised cantonal health authority can request the data or, if it wishes, access the data directly with a secure key.

The requirements of the authorities are thus fully complied with. You have helped to contain the pandemic, which is in the interest of all of us – you have saved time in the tracking process and restricted quarantines.

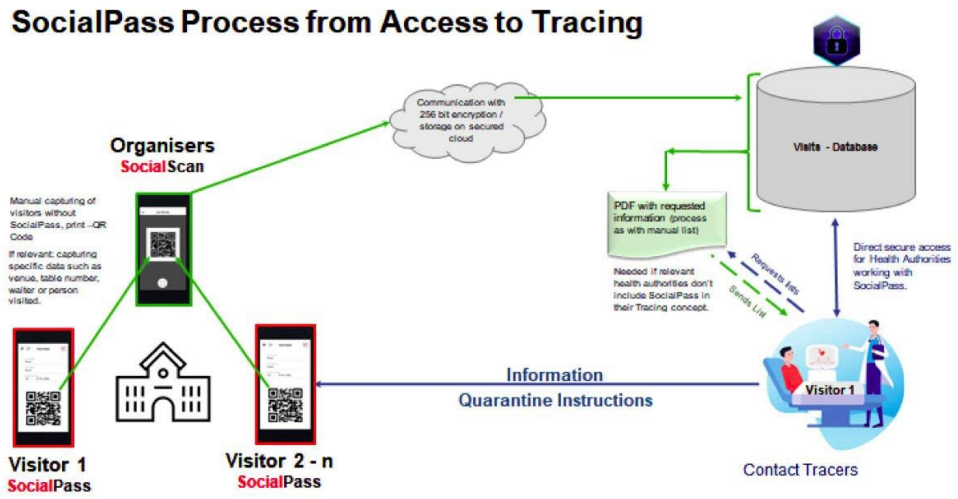
SocialPass is a free app

Perform STRIDE on the SocialScan system



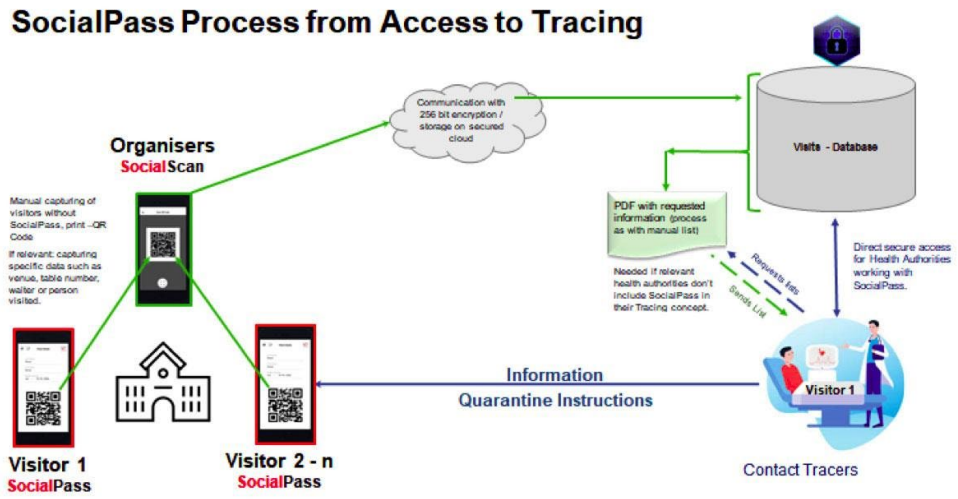
Perform STRIDE on the SocialScan system

Threat	Property threatened
Spoofing	Authenticity



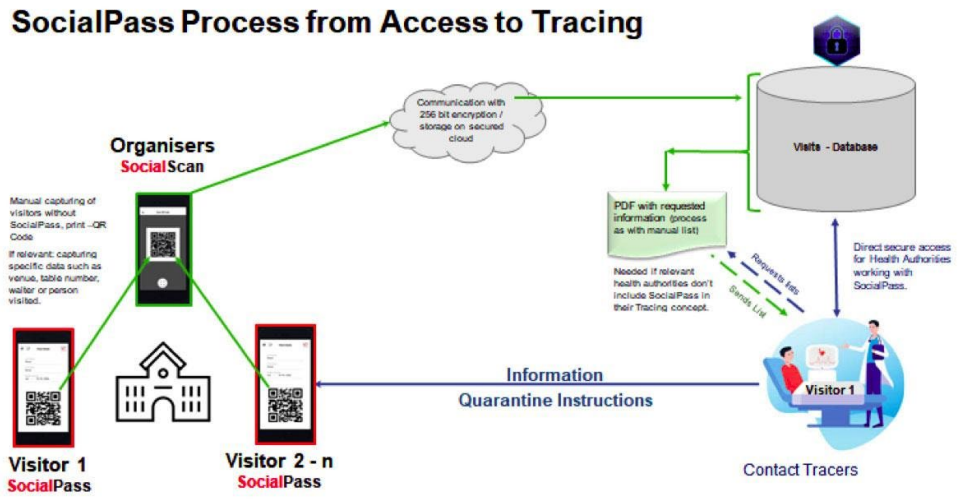
Perform STRIDE on the SocialScan system

Threat	Property threatened
Tampering	Integrity



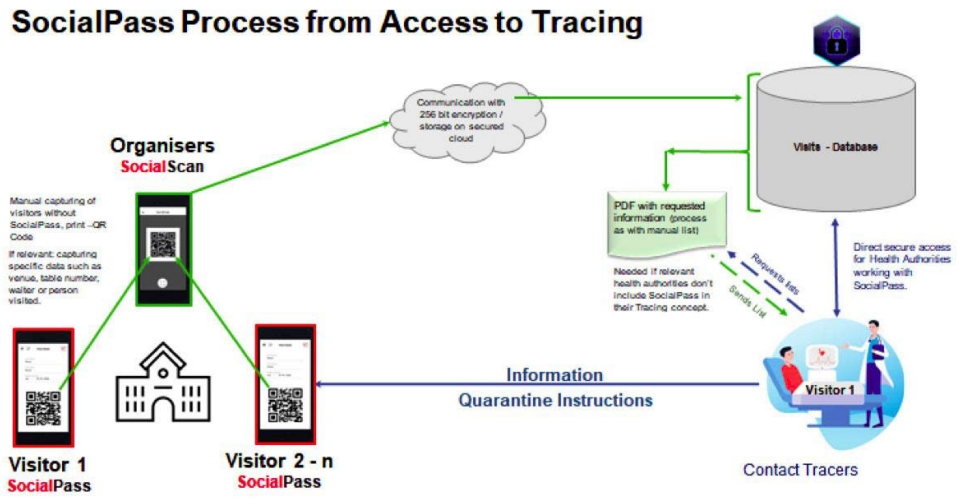
Perform STRIDE on the SocialScan system

Threat	Property threatened
Repudiation	Non-repudiation



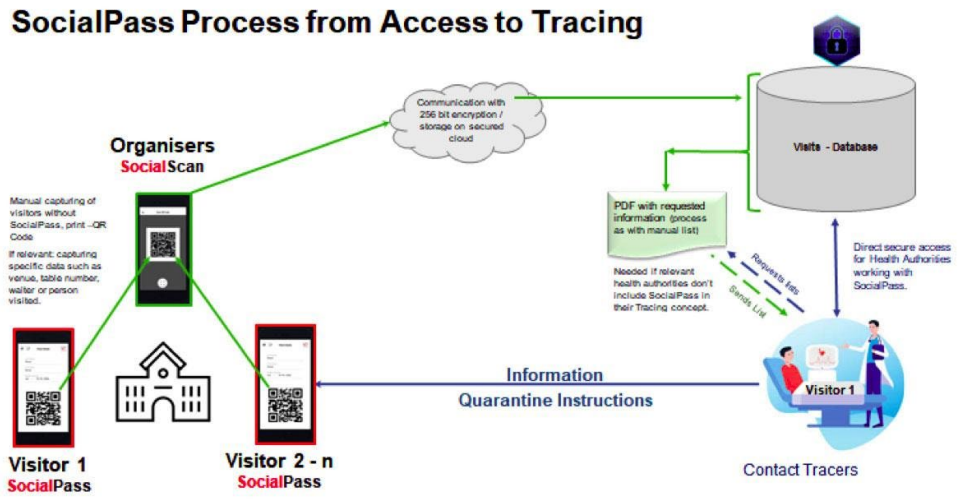
Perform STRIDE on the SocialScan system

Threat	Property threatened
Information disclosure	Confidentiality



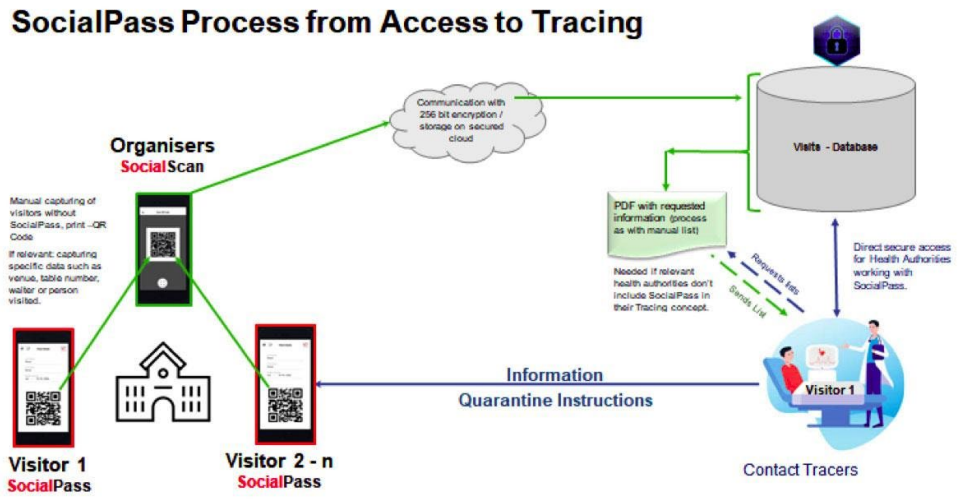
Perform STRIDE on the SocialScan system

Threat	Property threatened
Denial of Service	Availability



Perform STRIDE on the SocialScan system

Threat	Property threatened
Elevation of Privilege	Authorization



Gruthentication

Gru decides to build a homemade authentication system for his minions. Gru wants to try alternative approaches to passwords and listed four substitutes.

Minions are very friendly, and tend to hang out in big groups to party and eat bananas.

Which authentication method provides Gru with **the least** assurance of the identity of a Minion?

(a) User's behaviour

(b) Biometric

(c) User's social ties

(d) Smart cards

Token-based authentication

Are the following **True or False**?

The token-based authentication mechanism seen in the class, which authenticate users using something that they have, require:

(a) That the token knows the public key of the verification server

(b) That both token and verification server use the same hash function

(c) That the token and the verification server share a key

(d) That tokens delete their key after each verification