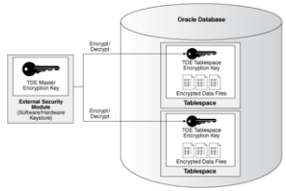
Computer Security (COM-301)

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.

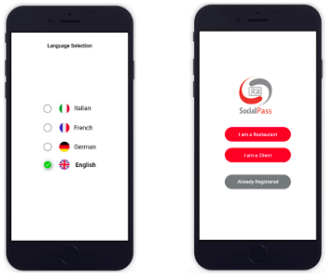
Propose a means for an adversary to obtain capabilities outside of this threat model

The capabilities that the adversary needs to acquire are credentials to login in the database, as that enables to decrypt.

Different means:

- Bribe an employee
- Corrupt/Hack the computer of an employee
- Threaten an employee
- Trick an employee to give you the credentials (social engineering)

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.

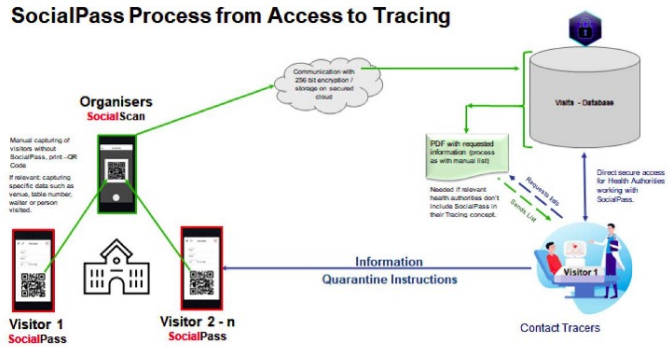
The data of your Pass will be stored directly in a secure "Swiss Cloud". **After 14 days they will be automatically deleted.**

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.

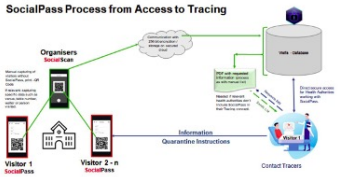
SocialPass is a free app

Perform STRIDE on the SocialScan system



Perform STRIDE on the SocialScan system

Threat	Property threatened
Spoofing	Authenticity



[Recall that these answers are not the only possible ones – see lecture video for more discussion: https://tube.switch.ch/videos/0239094c]

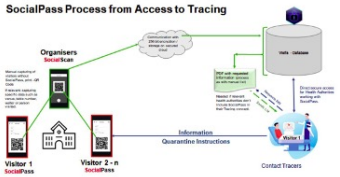
Spoofing is when someone or something pretends to be something else in an attempt to breach the security of a system.

In SocialScan, several parties could be spoofed. For example: :

- The users (through their phones): *check-in as other user*
- The organizer, when sending their information to the database: *can change the input (check others, delete checkins, checking in the wrong place)*
- The contact tracers, both when accessing the database, and when communicating with the visitors: *obtain check-in data on any restaurant. Tell users they are sick then they are not*

Perform STRIDE on the SocialScan system

Threat	Property threatened
Tampering	Integrity



[Recall that these answers are not the only possible ones – see lecture video for more discussion: https://tube.switch.ch/videos/0239094c]

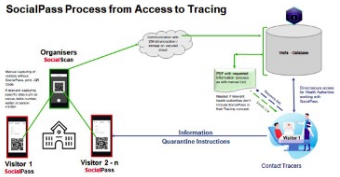
Tampering is when an adversary alters information stored or sent

In SocialScan, an adversary could tamper with, for example:

- Information on the phones: *to cheat the scanner*
- Information on the organizer's device: *to modify the data sent to the server*
- Information in transit from the organizer to the database: *to modify the data sent to the server*
- Information in transit from the database to the contact tracers: *to modify the list sent from the server*

Perform STRIDE on the SocialScan system

Threat	Property threatened
Repudiation	Non-repudiation



[Recall that these answers are not the only possible ones – see lecture video for more discussion: https://tube.switch.ch/videos/0239094c]

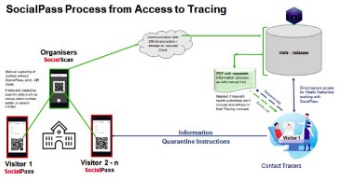
Repudiation is when a party denies having made an action in the system.

In SocialScan, several actions could be repudiated:

- The users could repudiate having shown a QR code
- The Organizer could repudiate having send information to the database
- The tracers could repudiate having accessed the database, or having communicated to a visitor

Perform STRIDE on the SocialScan system

Threat	Property threatened
Information disclosure	Confidentiality



[Recall that these answers are not the only possible ones – see lecture video for more discussion: https://tube.switch.ch/videos/0239094c]

Information disclosure is information in the system is made available to non-authorized parties.

In SocialScan, information could be disclosed from, for example:

- The users or organizer's devices: *the check-ins in those devices*
- In transit between organizer/tracers and database: *check-ins being sent*
- In transit between contact tracers and visitors : *check-ins being sent*
- The database : *check-ins in all restaurants*

Perform STRIDE on the SocialScan system

Threat	Property threatened
Denial of Service	Availability

[Recall that these answers are not the only possible ones – see lecture video for more discussion: https://tube.switch.ch/videos/0239094c]

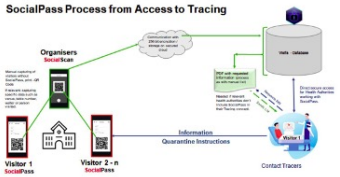
Denial of Service is when one or more part of the system are made unavailable.

In SocialScan, several parts could suffer a denial of service attack. For instance:

- Mainly the database (to prevent organizers from sending data, or the tracers form accessing)
- The users devices, so that they cannot receive information from the contact tracers

Perform STRIDE on the SocialScan system

Threat	Property threatened
Elevation of Privilege	Authorization



[Recall that these answers are not the only possible ones – see lecture video for more discussion: https://tube.switch.ch/videos/0239094c]

Elevation of privilege is when the adversary obtains more permissions than what they would be originally allowed.

In SocialScan, there is a risk of elevation of privilege, for instance:

- When accessing the database, an adversary could gain access to
    - Upload codes (e.g., an organizer being able to upload codes on behalf of an organizer)
    - Read entries (e.g., a contact tracer being able to read information from venues other than those categorized as dangerous)

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

Since the minions are always in groups, their social ties are not very unique. Answer: (c)

(a) could be argued for by minion experts (which are not) if they all behave the same, compared to potentially several groups.

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

(a) **False**: token-based authentication uses symmetric cryptography. There is no public key

(b) **False:** the token requires a shared secret that is input to a keyed cryptographic function. A hash does not work. Otherwise anyone could compute new values after seeing one output from the token.

(c) **True:** the token and the server do need to share a key to be able to compute the same values

(d) **False**: if tokens delete the key after verify, then they cannot compute further verification values