KFUPM
College of Computer Science and Engineering
Computer Engineering Department
COE 426/526: Data Privacy

Fall 2020 (201)

Assignment 4: Due date Saturday 15/12/2020

Tasks

Q1: (10 points) Tor is an overlay system for increasing anonymity and circumventing censorship on the internet. Tor can be used to anonymise browsing of the regular World Wide Web. Using resources available on the Internet, answer the following questions.

(a) How does Tor anonymise the browsing?

(b) How does Onion routing work? i.e. What happens while a message travels across the Tor network

(c) In addition to regular WWW, Tor can be used to access so called hidden services. How are they different from browsing regular WWW sites?

(d) Tor provides anonymity. Does it also mean security? How can anonymity get compromised on Tor?

Q2: (15 points) Contact Tracing applications played an important role in controlling the spread of COVID-19. Like any other technology, contact tracing applications are susceptible to a large array of attacks that can compromise the security and privacy of the patients data. Using available resources in the Internet (few examples of articles and papers below), answer the following questions.

(a) What are the PIIs in contact tracing applications? Who are the stakeholders?

(b) List three types of attacks that can compromise the privacy of PIIs?

(c) For each listed attack in the Task (b), propose an appropriate privacy-enhancing technology to mitigate the risk of such attack.

(References)

- A Survey of COVID-19 Contact Tracing Apps (https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=9144194)
- COVID-19 contact tracing apps: a stress test for privacy, the GDPR, and data protection regimes (https://academic.oup.com/jlb/article/7/1/lsaa034/5848138)
- COVID-19 Contact tracing: data protection expectations on app development (https://ico.org.uk/media/for-organisations/documents/2617676/ico-contact-trac
pdf)