Introduction to IoT: Autumn 2019

Exercise set: 6

Due on 16th October 2019 by 16:00.

Instructions: All course participants are requested to submit their exercise solutions (in English) electronically to the instructors Agustin Zuniga (agustin.zuniga at helsinki.fi) and Prof. Petteri Nurmi (petteri.nurmi at cs.helsinki.fi) by the due date. Use the following subject in your email: *IoT_week[#]_[last name_first name]_[student number], (i.e. IoT_week6_Zuniga_Agustin_12345)*

Your submission have to contain no more than **(four 4)** single-spaced and numbered pages. Use font type Arial or its equivalent with size no smaller than 10 points. Include the exercise set number, your full name and student Id in the upper right corner of the first page.

In all the exercises, do not just give the answer, but also the derivation how you obtained it. Participants are encouraged to review course material to answer the problems and in some cases write computer programs to derive solutions.

Learning objective: In this set of exercises you will understand how privacy and security perform in *IoT* contexts. The tasks will help you to clarify the difference between privacy and security, and the considerations you should take into account when implementing IoT applications.

Task 1 (2 pts.)

Choose one of the applications at the bottom and answer the following questions:

1. What privacy risks and attack types would the application have and why? Cite at least one risk and one type of attack to get full points.
2. Which privacy enhancing technologies (PETs) would you use to mitigate these issues?

Application 1: A car manufacturer has added IoT features on its vehicles. Specifically, its cars use IoT-based intelligence to improve driving quality and safety while driving. One of the functions includes periodically collecting data while the vehicle is being operated. The data include information like remaining gas, time when it has been driven, route it has taken, number of persons in the vehicle and driver profile. Drivers can access this data locally to know the current driving conditions including speed, location and traffic. Additionally, data is sent to the back-end of the manufacturer to evaluate the performance of the components in the vehicle, to assess they could be improved in upcoming models, and to inform the driver of potential faults in the car.

Application 2: Besides of having a temperature sensor, Xin's fridge includes features like touchscreen interface, microphone, internal camera and RFID reader. Before going home, Xin gets a reminder that the milk in his fridge expires soon. At the supermarket, Xin uses his mobile to connect to the internal camera of the fridge and checks if there is something else he should buy.

Identity	Alias	Identity	Marital Status	Occupation	Gender	Weight(Kg)	Heigh(cm)	Universe
Bruce Wayne	Batman	Secret	Single	Businessman	Male	95	187	DC
Barry Allen	The Flash	Secret	Single	Scientist	Male	88	182	DC
Ollie Queen	Green Arrow	Secret	Single	Businessman	Male	80	178	DC
Alan Scott	Green Lantern	Secret	Married	Adventurer	Male	91	182	DC
Clark Kent	Superman	Secret	Married	Reporter	Male	107	191	DC
Diana of Themyscira	Wonder Woman	Secret	Single	Adventurer	Female	75	182	DC
Kate Kane	Batwoman	Secret	Single	Business woman	Female	66	180	DC
Arthur Curry	Aquaman	Public	Engaged	Adventurer	Male	147	185	DC
Peter Parker	Spiderman	Secret	Single	Photographer	Male	76	177	Marvel
Steve Rogers	Capitain America	Public	Single	Adventurer	Male	100	187	Marvel
Tony Stark	Ironman	Public	Engaged	Businessman	Male	102	185	Marvel
James Howlett	Wolverine	Public	Divorced	Adventurer	Male	136	182	Marvel
Carol Danvers	Capitain Marvel	Public	Single	Adventurer	Female	56	180	Marvel
Natalia Romanova	Blackwidow	Public	Divorced	Secret Agent	Female	57	170	Marvel

Table 1

Task 2 (4 pts.)

Consider the information given in table 1 to do the following:

1. Apply pseudonymisation to prevent identity and occupation of the superheroes being revealed. Describe the method you use and include one example.
2. Apply 2 and 3-anonymity to prevent identity of the superheroes being revealed. For each *k*, show one case where de-identification can re-identify the name.

Task 3 (4 pts.)

Find a news article about an IoT vulnerability being exploited

1. What type of attack was performed?
2. What methods from the course slides could have been used to mitigate the attack in terms of privacy? Justify your answer to get the full points.
3. What methods from the course slides could have been used to mitigate the attack in terms of security? Justify your answer to get the full points.
4. Which IoT layers the attack focused on?

Bonus Task 1

Complete the IoT data privacy checklist for **Application 1** of Task 1. Refers to Lecture 11 of the course. Answer the 10 questions using the information about application functions. Assume the rest of the information necessary to fill the checklist.

Bonus Task 2

Use the following RSA public key to encrypt the phrase: Winter is coming!

Copy the encrypted message as part of your submission. Hint: There are online tools that offer free RSA encryption and decryption.

RSA public key: MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQC01E5yofIJ4N9wNXJ2Pkf RQcLOGBXV0tXSZ+LXPL7YZHRnxAsUN6FlYyxjHyFB+CdKVsziYjavZ9ipSCZOQlKDmIUaEdYf30

DFegEYsInpgsKsAAaDfVcT8QvMM5F57kyzW2d/dTOXF235YMvXVRSIbXbA63AQyqRtGXVRPVw7
cwIDAQAB

Bonus Task 3

Maria is having problems with her IoT application. The manufacturer asks her to collect and send some sensors' data. Use one of the methods from the course slides to check the integrity of the dataset sent by Maria and the one received by the manufacturer. Report the results of the integrity evaluation. The files are available through Moodle in Exercise 6 folder.