UNIVERSITETET I AGDER

KANDIDAT

217

PRØVE

DAT235 G Sikkerhet og IoT

Emnekode	DAT235
Vurderingsform	Skriftlig eksamen
Starttid	14.12.2017 08:00
Sluttid	14.12.2017 12:00
Sensurfrist	04.01.2018 00:00
PDF opprettet	17.11.2019 12:45

Oppgave	Tittel	Oppgavetype
☑	DAT235 G Generell informasjon	Skjema
1	DAT235 G Oppgave 1	Langsvar
2	DAT325 Oppgave 2	Langsvar
3	DAT235 Oppgave 3	Langsvar
4	DAT235 Oppgave 4	Langsvar

☑ # DAT235 G Generell informasjon

Emnekode: DAT235
Emnenavn: Sikkerhet og IoT

Dato: 14.12.2017
Varighet: 09:00-13:00

Tillatte hjelpemidler: All written material

Merknader:

Det forekommer av og til spørsmål om bruk av eksamensbesvarelser til undervisnings- og læringsformål. Universitetet trenger kandidatens tillatelse til at besvarelsen kan benyttes til dette. Besvarelsen vil være anonym.

Tillater du at din eksamensbesvarelse blir brukt til slikt formål?

Velg et alternativ

- ◉ Ja
- ○ Nei

Knytte håndtegninger til denne oppgaven?
Bruk følgende kode:

6 9 0 3 2 8 8

1 # DAT235 G Oppgave 1

Skriv ditt svar her...

1.1

Stikkord; (keeping data secret ,restricting read access)

- Data Confidentiality
  - Is the when you are making sure that only authorized persons have access to it.
  - Restricting it read access.
  - Keeping data secret
  - Data confidentiality is all about making sure that sensetive information about a person don't get's leaked. Like one's full name, housing information and credit card information.

1.2

- Entity Authentication.
  - A thing with distinct and independents existence.
    - Person or process to us (Humans)

1.3

- Authentication
  - How do we know that you are you
  - Authentication is about identifying yourself with something
    - What you know
      - Password
      - Pin Code
    - What you have
      - Security Dongle
      - ID Card
      - Mobile ID
    - What you are
      - Biometrics
- Authorization
  - Indicates what one is permitted to do..

1.4

Since we don't know what's going to happen, meaning that if we make the calculations that we are having a system that is risk free, doesn't mean that it's always going to be risk free, since the system is changing. the risk

is also changing then based on the system.

1.5

Terretorial Scope, is meant by scoping out the things that are in the terretorium, meaning

1.6

- Pretexting - A lie that makes the target assume things
  - Affects identification, authentication and authorization
  - Often relies on assumed associations
  - Often relis on your weaknesses (What you want to happend, want to hear)
  - Relies on misplaces trust in instututions, brands, etc

- Tailgating - Also called piggybacking
  - A person tags along with another person who is authorized to gain entry into a restricted area, or pass a checkpoint.
  - A persons swipes his card to walk though a gate, but 2 persons enter instead of 1.

1.7

- Major categories of physical threats
  - Extreme temprature
    - Servers overheating
  - Gases
  - Liquids
    -
  - Living Organisms
  - Projectiles
  - Movement
  - Energy anomalies
  - People
  - Toxins

    - Smoke and fire

1.8

1. **Remove unnecessary software**
    * Reduce attack surface
2. **Remove unneeded services**
    * Telnet, smtp...osv
3. **Alter default accounts**
    * System can have many default account for diffrent purposes
        * Must assume that these are well-known to attackers
        * Disable and remove that those you don't need
4. **Apply "least Privilege"**
5. **Apply updates (Use newest version whenever practical)**
6. **Implement logging and auditing**

1.9

It's secure :)

1.10

- Input Validation
    - Is checking that the information typed in corresponds to a valid form of response: if you have a function that adds 2 numbers together, then you want the intput to be a integer or a float, and would not want a string.
        - Advantage
            - You'll know for sure that you are getting the correct type
        - Disadvantage
            -
- Input Sanitation
    - is making sure that the whole input only does what it was intended for, whithin its intended funtion. an example could be that one uses a semicolon ";" to escape the current function to get a higher access, or access to another function which it should not have.
        - Advantage

    - you are somewhat certaint that hackers can't send code in forms that post something somewhere
- Disadvantage
    -

Knytte håndtegninger til denne oppgaven?
Bruk følgende kode:

7 1 0 4 8 9 9

2 DAT325 Oppgave 2

Skriv ditt svar her...

2.1.1

A model is a simplifiesd and abstract version of the modeled item. It should be kept simple when possible. (remove unimportant details) But, the essential elements must be there.

2.1.2

1. What are you building?
2. what can go wrong?
3. What are you going to do about it?
4. Check your model and your measures

2.1.3

- Defining assets
    - Something an attacker wants
    - Something you want to protect
    - A stepping stone towatds a) and/or b)

2.1.4

- Advantages
    - you will know how what threats that can occur
- Disadvantages
    - you migth not know how "deep" the threats are.. as you would

like

2.1.5

- Strategies for Dealing with identified threats
  - Are all threats addressed
  - Are he threats addressed in a satisfactory way
  - Are the addressing consistent

2.2)

When it came to the threath model of the system which contains a headset talking to a app which then again talks to a server.

- **S**poofing
  - Headset <- Bluetooth -> Phone
    - since this is wireless communication (bluetooth) with each of the devices, there is a chance that the communication stream could be spoofed, meaning one could listen to what one are listening to aswell picking up anything said close to the headsets microphone.
    - This meaning that the communication would be needed to encypted in a way so no one could just listen to it.
  - Phone <-- Wireless or Cell Data Link --> Cloud
    - this connection is also in danger of getting spoofed, like getting the username and password. and aswell looking at the other data comming from the connection
- **T**ampering
  - Headset
    - Tampering with the headset is possible, but one would be needing to get the headset without no one noticing it's gone, .. but could make it suspicious that it would have been tampered with that it litterally don't feel rigth.
  - Phone
    - You could tamper with the phone, install a backdoor when one isn't looking and getting more information of the phone

    - Cloud
        - if the cloud is properly secured it migth not be able to be tampered with, and even getting physical access to this server thats in the cloud can also be a way, but that though a bit harder to get, so i woudln't see this as a threat..
- **R**epudiation
    -
- **I**nformation Disclosure
    - Phone <-- Wireless or Cell Data Link -->
        - Since the information can eithe go over wireless og data link since the application don't care what kind of connetion it goes over. this can mean that information not meant to be shared is getting shared. like personal sensetive information
- **D**enial-of-Service
    - Cloud
        - The cloud server could be the target for a DDos or a denial of service attack, meaning that the phone would not be able to sync its data to the cloud which then could betyr at data is gettting lost.
- **E**levation of privilege
    - Phone
        - This migth be done with the phone if the message it's getting from the headset is containg some thing more rather than just the audio data,..you could inject or escape into a shell and execute commands installing a backdoor or giving access to do more over the bluetooth connection than what you should.
        - THis goes alos for the cloud server, that you migth tamper with the packets and send a packet containg something else rather than your info about what to sync... giving you a elevated shell to the server
        -

Knytte håndtegninger til denne oppgaven?

7 5 0 4 0 9 5

3 DAT235 Oppgave 3

Skriv ditt svar her...

3.1

A Real-Time Operating System or RTOS in short, is a operating system designed to run on Microcontrollers.

3.2

- Link Layer
  - Advantages
    - safety from node to node
  - Disadvantages
    - Information tracels more than one node-jump and link-laye security can't guarentee safety end-to-end

- Network Layer
  - Advantages
  - Disadvantages

- Transport Layer
  - Advantages
  - Disadvantages
    -

3.3

- Privacy Challanges
  - Keeping data Safe and secure.
  - make sure things don't get leaked un-intentionally.

3.4

- The PIA process is split into 4 main categories.
  - Project Initiation
    - This is the step where you define the scope of the PIA process (which caries by organization) If the project they are running is in early stages and detailed information is unknown the organization may choose to do a preliminary PIA and then a full PIA once it gets off the ground
  - Data Flow Analysis
    - This step involves mapping out the proposed business process as it regards personal information, identifying clusters of personal information, and creating a diagram of how the personal information flow through the organization as a result of the business activites in question
  - Privacy Analysis
    - This step requires all personell involved with the movement of private information to complete privacy analysis questionnaries, as well as secondary check-ins on the answers to the questionanaries wwhich require more detail, and discussion of the privacy issues and implication brought up as a result of the questionnaries
  - Privacy Impact Assessment Report
    - This step requires the organization to create a documented evaluation of the privacy risks and porential implications of said risks brought up by the outcomes of the previous steps, as well as discussion of possible efforts that could be made in order to mitigate or remedy the risks.

3.5

it means that one is informed by the consent of the user.,that you can't give out it's information without it's consent that it's okay..

3.6

To solve this problem, you could hash the password and the username

before itsbeing sent meaing that aynone listening in to the connection wouldn't neccessarily find it but, if found it would look like jibberish to a normal person. so when the connect package was recived at the server it would de hash the password and username, and then try to connect which would make it somewhat secure.

However another solution is to setup the communication with the client and the server on a vpn encrypted vpn connection, so it would be "hidden" in the packet logs..

3.7

It's benefits is that as an attacker you won't always know the mac address of a device if "MAC address randomization" is on. Meaning it will change it's Mac address to a random unkown Mac Address, instead of usings it default one.

3.8

- Vulnerability
  - A Vulnerability is a essentially a way to infiltrate a machine to gain access to either data or superusers.
- Threath
  - A Threat is something that migth appear as a way to gain access to a machine.
  - Example
    - A Server in a company migth be availiable inside and outside of the company's network, and the server cointains a lot of personal and sensetive information. Then this is a threat to the company as it's not secured enough...

3.9

One does simply not walk into mordor...

3.10

It was done by infecting a single device, and with that that device would infect anyone in a certain proximity range. Meaning so that you could infect a single device and put it up in a city, and it would more or less just infect everything.
So when Device A infected Device B.. Then Device B would infect anyone that was close to that and this is how it would just spread incredibly fast.

Knytte håndtegninger til denne oppgaven?
Bruk følgende kode:

3 9 5 9 3 4 7

4 **DAT235 Oppgave 4**

Skriv ditt svar her...

4.1.1

MQTT default port;1883

4.1.2

dat235/device_07/#
This will log everything from device_07, # is a wildcard used to match any numbers of levels whitin a topic tree, including the parent itself.

4.1.3

- Retained
  - indicates that the application message, must be stored in the

server and delivered to future subscribers of that topic.

4.1.4

- QoS 1 (At least once (1))
  - Sends it off, hope everything goes okay.
    - This benefits that can send one packet at least once, making less traffic.
    - Drawbacks is that if one of the packets gets lost, then you migth not know what happen to it.

Protocol Exchange QoS1

Client server protocol interaction

1. client --> Publish --> server
2. client <-- puback <-- server

- QoS 2 (Exactly once(2))
  - exactly one time it's certain that it'll arrive

Protocol Exchange QoS2

Client server protocol interaction

1. client --> publish --> server
2. client <--pubrec <-- server
3. client --> pubrel --> server
4. client <-- pubcomp <-- server

4.1.5

To look out for the last will ,I would subscribe to the last_will topic.

would use QoS 2, since one would like to be sure that the message did arrive and that we are sure that the device is not working properly.

i would use retained, due to if no one connected before it disconnected.. then it would be like that when someone connected it would send the retained to the client that connected.

4.2.1

- sudo apt-get update - Updates the repositories with the latest information about packages.
- sudo apt-get upgrade - will upgrade the installed packages in rasbian (and if one of the packages would break the system in some way it would ask you if you **really** want to do this)
- sudo apt-get dist-upgrade - will upgrade the version of rasbian, aswell as software that in the distrobution.
    - dist-upgrade = Distrobution Upgrade

4.2.2

- First make sure i'm in my home directory, by writing cd then enter.
- sudo chmod 600 personal-secrets.text
    - This would give the user read & write access on the file, and no other

4.2.3

The shebang is this **!#** it's being used in script files to tell what interpreter it should run as...

If you had a python script called Hello.py, and you tried running it as ./Hello.py it would not know what to do with it since it did not declare in the top what kind of interpreter it should run as. So if you decleared in the top !# /usr/bin/python2

it would then know that it should be runned with the python interpreter...

if you didn't have the shebang, you would have to run the script as python2 Hello.py

4.2.4

you would use the command change. Which is used to get users to edit their password in a certaint amount of time.

- change -u mordor -d 90 -w 21

This is what you would use to get the user mordor, to change it's password whent it's been 90 days since last password change. -w 21 is used to say that it'll give a warning in 21 days before the password should be changed.

4.2.5

Rasbian is a operation system based of the popular linux-distro Debian, customly made to run on the raspberry pi.
(When i say customly, I mean the norwegian phrase"skreddersydd")

Knytte håndtegninger til denne oppgaven?
Bruk følgende kode:

9 1 8 7 9 1 6