Fundamentals of System Security (COMSM0122)
Group Assessment
(31st October, 2022)

Systems Security Design

Sceanario

EnA is a software-supported system that enables low-income and vulnerable households to achieve energy use efficiency in their homes. This is achieved using a mobile app that provides homeowners end-to-end service brokering. . The system components include:

1. `Homeowner Authentication System (HAS)`: Generates a personal passport that the homeowner can use to leverage EnA services.

2. `Home Identification System (HIS)`: Generates a home passport that contains unique features of a home associated with a homeowner.

3. `Home Assessment Manager (HAM)`: This component links homeowners to home energy efficiency assessment providers. HAM operates by broadcasting an assessment request containing a home passport to all home energy assessment providers registered with HAM. Assessment providers may then respond with a quote and timeframe to carry out the assessment. AHM then compares all quotes to select a preferred assessment provider. A chosen provider uses a home passport to generate an energy efficiency report. The report contains information that enables homeowners to be aware of energy-inefficient sections of their home that could benefit from a retrofit and associated costs. This allows homeowners to make an optimal decision on which sections in their home to retrofit in order to increase energy efficiency.

4. `Retrofit Financing (RF)`: This component enables homeowners to prudently finance a retrofiting activity. This is done by linking homeowners to different financial options, enabling them to aggregate various financial streams to support a retrofiting activity. RF operates by matching both personal passport from HAS and retrofit option from HAM with grants provided by government agencies and low-cost finance schemes from banks. A match result contains the amount of money in government grants and/or bank loand that the homeowner can leverage to support the retrofit option. Note that a bank may further disclose the personal passport from RF to credit referencing agencies to acertain the credit worthness of the homeowner. The homeowner selects a match and agrees to proceed with a financed retrofit job.

5. `Retrofit Contracting (RC)`: This component links homeowners to qualified contractors who carry out an agreed retrofit job. RC achieves this by maintaining a

datastore of approved contractors. It recommends a suitable contractor based on a retrofit job, cost and the experience of the contractor.

Figure 1 is a high-level system architecture showing data-flows between service components. EnA integrates with government supported agencies such as Green Homes Grant and winter fuel allowance, as well as leverage services from most credit unions and building societies. The current customer base consists of about 50,000 households, and most of its accredited contractors are specialists in loft insulation, double-glazed windows and solar water heating systems. The growth plan is to scale up its customer base to 100,000 by leveraging more financial service providers. EnA also plans to provide other services targeted towards middle and high-income households. A data analyst to help achieve its growth plan was recently onboarded. EnA uses a single datastore `homeowners.json` to satisfy all its operational and analytical requirements

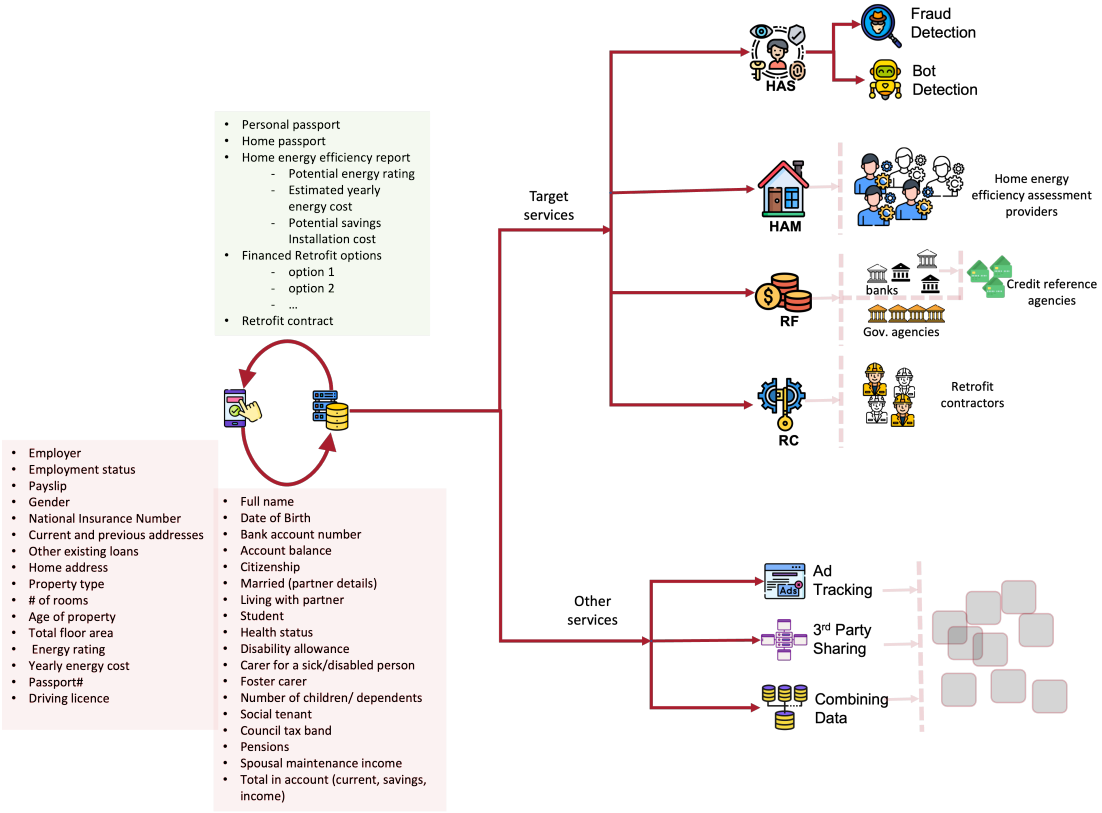

Figure 1: Systems Architecture showing data-flows between EnA service components.

Execute tasks 1-4 based on described scenario, each task carry 10 marks.

Task 1(10 Marks):

With increasing customer-base, EnA is also experiencing influx of houseowner Subject Access Request - the right given to a customer by law to obtain a copy of their personal data, as well as other supplementary information. There is a high risk that EnA will

Table 1: Data Sensitivity Labels

Level	Tag	Description
Highly Sensitive Data	hsi	Data that can personally identify an individual and is highly sensitive if disclosed, such as national insurance numbers, health data and financial data.
Sensitive Data	si	Data that can personally identify an individual
Quasi Sensitive Data	qsi	Data that can identify an individual when combined with other data
Low Sensitive Data	lsi	Data that is relatively harmless

incur regulatory fines, given its poor monthly access request to fulifilment ratio of 0.5%. On a deeper review of EnAs architecture, it was discovered that data from homeowners was being shared and processed by significantly high number of service components. Some services were not directly under control of EnA, and in certain cases changed the nature of data they consumed. This made it difficult to satisfy subject access request at scale or even acertain whether a specific service consumed data from a homeowner.

1. Based on Figure 1, which EnA service components are more likely responsible for the low access request to fulfilment ratio?

2. Propose a refactoring of EnA system architecture in Figure 1 that addresses highlighted problem. Explain your design rationale in no more than 150 words.

3. There have been reports of phishing attacks on homeowners from fraudulent home energy assessment providers. To address this problem, a decision has been made to change the design of how HAM interacts with energy assessment providers.

   (a) In no more than 150 words, discuss why the current design of HAM may be less trustworthy.

   (b) In no more than 150 words, discuss two alternative ways that HAM can interact with energy assessment providers.

Task 2(10 Marks):

As the systems security engineer, you've been tasked to operationalise a data tagging strategy for EnA datastore using data sensitivity labels shown in Table 1.

1. For each field in `homeowners.json`, generate a tag matching the regular expression:

```
(business|personal):[a-z]+(-[a-z]+)*
```

A tag should enable the identification of the sensitivity level of its associated field, and also computationally distinguish between house, demographic, healthcare and financial data. Use the template in Table 2, and where necessary provide comments justifying your tagging.

Table 2: Field tags based on sensitivity levels

Field	**Tag**	**Comments (optional)**

2. Based on Task 2.1, implement a function `tagHOFields()` in the file `HODTagger.js` to automatically assign tags to each field type in `homeowners.json`. Save the new json object as `taggedhomeowners.json`

3. Implement the function `profileHOFields()` in the file `HODTagger.js` to determine the sensitivity profile of taggedhomeowners.json. The function should provide insights on the percentage of records that are in each sensitivity class as well as the sensitivity of medical, demographic, house and financial data.

   (a) What proportion of `homeowners.json` is highly sensitive data.

   (b) What proportion of `homeowners.json` is sensitive data.

   (c) What is the sensitivity distribution of financial data in `homeowners.json`.

   (d) Define data protection policies for `homeowners` datastore.

Task 3(10 Marks)

Introduce a new data pipeline that enables varying access control, sharing and retention policies. Write a function `createNewDatawarehouse()` in `HODTagger.js` that will generate four new datastores from `taggedhomeowners.json` as follows:

1. A datastore named `homeowner-m.json` that only contains medical records.

2. A datastore named `homeowner-h.json` that only contains home records.

3. A datastore named `homeowner-f-f.json` that only contains financial + fullname records.

4. A datastore named `homeowner-m-a-d.json` that only contains medical + address + demographic records.

Discuss the data protection risk associated with this new data pipeline, including how such risk can be mitigated.

Task 4(10 Marks)

Assume the capability of the analyst onborded to help EnA achieve its growth plan is defined in an access control matrix as follows:

	`homeowner-m`	`homeowner-h`	`homeowner-f-f`	`homeowner-m-a-d`
Analyst		r	rw	r

Where: r - read, w - write

	Security Label
Analyst	si

Security labels of subject: hsi > si > qsi > lsi

	Security Label
`homeowner-m`	hsi
`homeowner-h`	lsi
`homeowner-f-f`	hsi
`homeowner-m-a-d`	hsi

Security labels of objects: hsi > si > qsi > lsi

1. Using Bell-Lapadula model, fill out the following table to specify readable and writeable objects of the analyst.

	Readable	Writable
Analyst		

2. Based on Task 4.1, assign a risk profile to the analyst as a proportion of sensitive or highly sensitive information that he/she can read.

3. Does the analyst require a write access to `homeowner-f-f`? Justify your answer in no more than 150 words.

Deliverables

Submission should be made electronically as a folder containing all deliverables via Blackboard for Groupwork. Your folder should be named `group-[your group number]`. The folder should contain the following:

1. A pdf document containing your answers for Tasks 1-4. State group name and its members including registeration number at the top of the document.

2. All new datastores from tasks 2 and 3.

3. Updated `HODTagger.js`

One member of a group may submit on behalf of the whole group. Every member of the group is expected to submit an individual reflective log (max. 500 words).

Assessment

Submissions is due by **13.00** on **3rd November 2022**. As per the Code of Assessment policy, information on late submission penalties can be found at:`https://www.bristol.ac.uk/students/support/academic-advice/outcomes/mark-signals/`. All submissions will be checked against our plagiarism monitoring system.

Dr Inah Omoronyia, MVB 2.39a Department of Computing Science, University of Bristol