UNIVERSITY of York

MSc/MEng/MMath Degree Examinations 2017/18

DEPARTMENT OF COMPUTER SCIENCE

Topics in Privacy & Security (PSEC)
Open Individual Assessment

Issued: Wednesday, 7th February, 2018

Submission due: 12 noon, Wednesday 14th March, 2018

Feedback and marks due: Wednesday 25th April, 2018

All students should submit their answers through the electronic submission system:

http://www.cs.york.ac.uk/student/assessment/submit/

by **12 noon, Wednesday 14th March, 2018**. An assessment (or part of an assessment) submitted after this deadline will be marked initially as if it had been handed in on time, but the Board of Examiners will normally apply a lateness penalty to the whole assessment.

The feedback and marks date is guided by departmental policy but, in exceptional cases, there may be a delay. In these cases, all students expecting feedback will be emailed by the module owner with a revised feedback date. The date that students can expect to see their feedback is published on the module descriptor:

https://www.cs.york.ac.uk/modules/psec.html

Your attention is drawn to the section about Academic Misconduct in your Departmental Handbook:

https://www.cs.york.ac.uk/student/handbook/

Any queries on this assessment should be addressed to Dr Radu Calinescu, radu.calinescu@york.ac.uk

Answers that apply to all students will be posted on the PSEC VLE page.

Rubric

Answer all questions. Note the page limits for each question. Parts of answers that go beyond the page limit may not be marked. References must be listed at the end of the document and do not count towards page limits.

Your exam number should be on the front cover of your assessment. You should not be otherwise identified anywhere on your submission.

General Marking Criteria

You will be given credit for clear and concise descriptions, and for organising your assessment into well-defined, meaningful sections.

Demonstration of appropriate research is expected for all parts of the assessment. You should cite relevant published work to support your statements and arguments throughout your assessment. Failure to demonstrate such research will lead to a loss of marks.

Question 1: Ransomware [60 marks]

In recent years, ransomware has seriously impacted key services and organisations [1,2]. The May 2017 WannaCry cyberattack alone has affected over 200,000 computers across numerous countries, including many computers supporting the delivery of healthcare services in the UK [3].

For this question, assume that you are a security consultant hired by a healthcare organisation concerned about the risk of future ransomware attacks. Your role is to help the organisation improve their personnel's awareness of ransomware risk, prevention and response.

technical report for IT Managers

(i) **[30 marks]** Write a technical report informing the organisation's IT managers about the structure of ransomware attacks, about the dangers these attacks pose to healthcare providers, and about the prevention, detection and response mechanisms they should implement on the organisation's computers to best protect them against such attacks.

Explain to non-technical users

(ii) **[20 marks]** Write a memo that the IT managers should email to healthcare personnel who are not IT experts, to warn them about ransomware, to inform them about ways to prevent ransomware attacks, and to advise them what to do if they are affected by such an attack. The memo must only cover the personnel's use of computers belonging to the organisation and located on the organisation's premises.

Justify non-tech explanation

(iii) **[10 marks]** Write a justification for the information included in the memo from part (ii) of the question, and for how you organised this information. The aim of this justification is to convince the IT managers that the memo they will send is going to be effective.

In answering each part of the question, consider the level of IT expertise of the personnel that your answer is aimed at, and the security mechanisms they are able to implement.

Your answer to this question must not exceed six A4 pages (minimum font size 11pt) plus references.

References

1. Cath Everett, 'Ransomware: to pay or not to pay?' *Computer Fraud & Security* 2016, Issue 4, pages 8-12, 2016. https://doi.org/10.1016/S1361-3723(16)30036-7. Last accessed 17 November 2017.
2. Krishna Chinthapalli, The hackers holding hospitals to ransom. BMJ 2017;357:j2214 doi: 10.1136/bmj.j2214, 2017. http://www.bmj.com/content/bmj/357/bmj.j2214.full.pdf. Last accessed 17 November 2017.
3. UK National Audit Office, 'Investigation: WannaCry cyber attack and the NHS', Report by Sir Amyas Morse, NAO Comptroller and Auditor General, 24 October 2017. https://www.nao.org.uk/wp-content/uploads/2017/10/Investigation-WannaCry-cyber-attack-and-the-NHS.pdf. Last accessed 17 November 2017.

Question 2: Trust-Enhanced Reputation Metrics [40 marks]

Online reputation systems are used to develop trust among the users of ecommerce and other online services [1]. Major providers of such services, such as Amazon, collect customer ratings of products, and use *reputation metrics* to derive measures of reputation from these data.

This question is concerned with evaluating the effectiveness of different reputation metrics for *discrete-valued rating systems*. These are systems in which customers rate products on an integer scale between 1 and *MAX_RATE*, where 1 represents the worst rating and *MAX_RATE>1* represents the best rating. An example is the Amazon product rating system, for which *MAX_RATE* = 5 (stars).

A frequently used reputation metric for these systems is the arithmetic mean: given a product j that was evaluated by a set of customers C_j such that the rating provided by customer $i \in C_j$ is x_{ij}, the overall product rating is calculated as:

equally weights genuine + fake reviews

$$r_j = \frac{\sum_{i \in C_j} x_{ij}}{|C_j|} \quad (1)$$

where $|C_j|$ represents the number of elements in the set C_j. This reputation metric has the disadvantage that it does not differentiate between customer ratings. Therefore, fake ratings from customers who create new accounts to promote their own products or to lower the rating of competing products are given the same weight as genuine ratings from long-established customers.

Trust-enhanced reputation metrics [2] mitigate this vulnerability of simple reputation metrics to *self-promoting* and *slandering attacks* [3] by associating a trust level $t_i \in [0, 1]$ with each customer i. The trust levels are then used to calculate the rating of product j as:

Binary trust level: aim to ignore slandering & self-promoting reviews

$$r'_j = \frac{\sum_{i \in C_j} t_i x_{ij}}{\sum_{i \in C_j} t_i} \quad (2)$$

so more weight is given to ratings from "trusted" customers.[1]

Your task is to design and implement a simple software tool for analysing the effectiveness of a trust-enhanced reputation metric that uses the following definition for the trust level t_i of customer i:

$$t_i = \frac{1 + \sum_{j \in P_i} f(r'_j, x_{ij})}{2 + |P_i|} \quad (3)$$

where P_i is the set of products rated by customer i, and

$$f(r'_j, x_{ij}) = \begin{cases} 1, & \text{if } |\, r'_j - x_{ij} \,| \leq \alpha \\ 0, & \text{otherwise} \end{cases} \quad (4)$$

[1] Note that setting all trust levels t_i to 1 in eq. (2) yields the arithmetic mean as in eq. (1).

Note how the value of function *f* is 1 if customer *i*'s rating of product *j* is no more than α away from the overall rating of the product, and 0 otherwise. The parameter α>0 specifies how far from the overall rating a customer's rating can be before it is deemed "dishonest". The tool shall take as input:

1. The value of *MAX_RATE* (a positive integer number);
2. The value of the parameter α (a positive number such as 0.5 or 1.2);
3. The name of a file containing a sequence of product ratings (one rating per line) in the format:

   `i j` x_{ij}

   where *i* is a customer ID (a positive integer number), *j* is a product ID (also a positive integer number) and $x_{ij} \in \{1, 2, \cdots, MAX\_RATE\}$ is customer *i*'s rating of product *j*.

The tool shall output:

1. The overall rating r'_j from eq. (2) and the arithmetic mean r_j from eq. (1) for each product whose ID *j* appears in the input file (in the format '`j` r'_j `(`r_j`)`', one product per line);
2. An empty line (to separate the two parts of the output);
3. The trust level (3) of each customer whose ID appears in the input file (in the format '`i` t_i', one trust level per line).

The overall product ratings and customer trust levels shall be accurate to two decimal places; and shall be those calculated after all individual ratings from the input file were processed. Note that processing an individual rating '`i j` x_{ij}' from the input file requires:

- If this is the first rating from customer *i*, using eq. (3) to initialise the trust level of customer *i* with the value corresponding to $P_i = \{\}$ (i.e. the empty set);
- Using eq. (2) and the current trust levels of the relevant customers to calculate the overall rating for product *j*;
- Using eq. (3) to update the trust levels of all customers who provided ratings for product *j* so far;
- Recalculating the overall ratings for the products – other than product *j* – affected by this updating of trust levels.[2]

Write a report covering the following aspects of your development and use of the tool:

(i) **[5 marks]** Describe how the tool works (e.g., by means of pseudocode accompanied by a suitable description), explaining how your design takes into account scalability issues (so the tool can handle large input files).

(ii) **[15 marks]** Use your tool with *MAX_RATINGS*=5 to analyse the effect of using α=1, α=1.5, α=2 and α=5 on the overall product ratings and on the customer trust levels for the sequence of individual product ratings from the input file `Q2Ratings.txt`, which is available in the 'Assessment/2017-18 Open Assessment Files' area on the module VLE. Include in your report: screenshots of

[2] Not recalculating the overall rating for product *j* avoids an infinite sequence of product rating and trust level updates.

the tool output; and plots of the overall ratings of the products with IDs 4, 7 and 29 for these α values. Discuss the differences between the results obtained for different α values, and between these results and the results obtained for the arithmetic mean.

(iii) **[10 marks]** Simulate a self-promoting attack to improve the rating of the product with ID 4 by adding *n* fake top ratings for this product at the end of `Q2Ratings.txt` from part (ii) of the question. Each such rating should have a new customer ID, corresponding to a new customer account created by the attacker(s). Plot the *increase in the overall rating* achieved by attacks of size *n*=5, *n*=10, *n*=15, *n*=20 and *n*=25 for the four α values from part (ii) of the question and for an overall rating based on the arithmetic mean. Repeat the experiments for slandering attacks on the product with ID 29, plotting the *decrease in the overall rating* achieved by slandering attacks of size *n*=5, *n*=10, *n*=15, *n*=20 and *n*=25 for the four α values from part (ii) of the question and for an overall rating based on the arithmetic mean.

(iv) **[10 marks]** Discuss the results from part (iii) of the question. Explain what value of the parameter α offers the best protection against the attacks you experimented with, and assess the advantages and disadvantages of different values for α.

Your report should not exceed four A4 pages (minimum font size 11pt), not counting the screenshots and plots from parts (ii) and (iii) of the question, and not counting the references.

You must attach as an appendix to your **single-file submission** the source code for the tool. If needed, use a ZIP archive to submit all components of the assessment as **a single file**.

Notes:

- Use a programming language of your choice to implement the software tool.
- Use a software application of your choice (e.g., Microsoft Excel) to generate the plots.

References

1. Paul Resnick, Ko Kuwabara, Richard Zeckhauser and Eric Friedman, “Reputation Systems”. In: *Communications of the ACM,* vol. 43, issue 12, pages 45-48, December 2000. Available online (only from the university network) at http://dl.acm.org/citation.cfm?id=355122. Last accessed on 17 November 2017.

2. Q. Feng, L. Liu and Y. Dai, “Vulnerabilities and Countermeasures in Context-Aware Social Rating Services”. In: *ACM Transactions on Internet Technology*, vol. 11, issue 3, January 2012. Available online (only from the university network) at https://dl.acm.org/citation.cfm?id=2078319. Last accessed on 17 November 2017.

3. Kevin Hoffman, David Zage and Cristina Nita-Rotaru. A Survey of Attack and Defense Techniques for Reputation Systems, *ACM Computing Surveys*, vol. 42. no. 1, December 2009. Available online (only from the university network) at http://dl.acm.org/citation.cfm?id=1592452. Last accessed on 17 November 2017.