University of BRISTOL

Systems Security

COMSM1500

bristol.ac.uk

University of BRISTOL

Preparing for the exam

bristol.ac.uk

Exam structure

- 40% of your unit grade
- 3 parts
  - Definition 30%
  - Problem 30%
  - Essay 40%

Definition example

c. Give an example of a threat to a web browser against which TLS does not protect you.

(5 marks)

Problem example

Question 1

Robert "Bobby" Tables works as a database administrator at Unsafe Inc. One day, just before lunch he gets a call from "John, Director of Marketing" who says he is at an important meeting with a customer in the U.S.A.. He has lost his company smartphone so he's bought a new one but can't remember his password: could Robert look it up for him in the company database? Robert initially refuses and the caller shouts at him over the phone that he'll get him fired. Robert remembers the last time he refused a request from management because it was against company policy, he almost lost his job (and missed out on a promotion, he thinks) over the matter. He apologises profusely, looks up the password in the database and reads it out to the caller: "ph0neWizard1".

Only minutes later, Robert sees the real John at lunch and realises that he gave his password out to the wrong person!

a. Identify two different vulnerabilities in Unsafe Inc., one technical and one organisational, that the attacker exploited in this situation.

(8 marks)

b. For each of the two vulnerabilities, describe what Unsafe Inc. should do about them and why.

(10 marks)

c. A systems thinker might say that in this situation, it would be wrong to punish Robert. Why?

(7 marks)

Essay example

Question 3

Write an essay on **one** of the following topics. This question is worth 40 marks. For all topics, the following are examples of writing that will get you marks: defining the key terminology and/or organisations involved, relevant examples, comparing and contrasting with other "solutions" in the same area, critical thinking, providing your own opinions with some justification.

a. Mozilla's Let's Encrypt (letsencrypt.org, officially launched April 2016) is the first free-to-use certificate authority.

   Explain the role of Certificate Authorities (CAs) and their certificates in the TLS protocol. In particular, give the relevant security aims and give your own opinion on whether these aims are being achieved. Explain how Let's Encrypt fits into this picture.

b. Ransomware is one of today's big security problems (Symantec called it "the most dangerous cyber threat" in September 2016). Although the idea is older, it has become increasingly prevalent since around 2010.

   Write an essay on ransomware, including an explanation of how it works and what kind of environment it needs to be successful. You may wish to consider the following questions: why is it such a problem today when it was fairly unknown 20 years ago? In what way are protections built against previous generations of malware often ineffective against ransomware? What might operating systems of the future do differently to mitigate the threat?

How to prepare for definitions

- Simply repeat knowledge from the course
  - What is X?
  - How does Y work?
  - etc…
- Go through the lectures video/slides
  - Identify key terms/technology/topics
  - Write a note card
  - … or whatever works for you

How to prepare for problems

- There will be a description of a situation, potentially inspired from a real life example
- On a topic seen in lecture
- You may be asked to
  - Identify a vulnerability in the approach taken
  - Identify a counter-measure
  - Identify a mean to detect an attack
  - Identify a better design for the system

How to prepare for problems

- Go through the lectures video/slides
  - Identify system design
  - Pay particular attention to lectures where “protocols” are described
    - e.g. TLS, TOR, signature scheme, proof of work etc…
  - Identify the “careful do not do that part of the lecture”
    - e.g. network authentication replay attack
  - Build complex note card about protocols/scheme/model/design we discussed
    - How it works
    - Why it works
    - What happens when you do not implement it properly

How to prepare for the essay

- There will be 3 topics choice
- Select wisely
  - Not necessarily what you think is “easier”
  - Pick a topic you are comfortable with
  - … and where you can demonstrate the breadth of your knowledge
- This is close to the reflective part
  - Why
  - How
  - Give examples

How to prepare for the essay

- For each lectures
  - Identify the main topic
  - Prepare discussion points around that topic
    - It is made quite explicit in most lecture
    - The extra-reading should also be a good hint
  - Identify examples
    - Where the techniques have been used?
    - Is there vulnerabilities?
    - How to prevent vulnerabilities?
    - Why does it happen?
    - etc…
- Again reflection part of you report should be a good preparation
- You obviously do not need to remember citations ;-) just explain

How to prepare for the essay

Mozilla's Let's Encrypt (letsencrypt.org, officially launched April 2016) is the first free-to-use certificate authority.

Explain the role of Certificate Authorities (CAs) and their certificates in the TLS protocol. In particular, give the relevant security aims and give your own opinion on whether these aims are being achieved. Explain how Let's Encrypt fits into this picture.

How to prepare for the essay

- Thifs is not necessary
  - For students who wants to learn more about security
- To find out about hot topics, read paper from:
  - USENIX Security
  - ACM CCS
  - IEEE S&P
  - NDSS
- http://csrankings.org
  - Good tool to identify top conference in a field
  - It is always debatable etc…
  - … but a good start

University of BRISTOL

Ask questions

Now is your last opportunity

Ask questions

- Go through the slides
  - https://github.com/bris-sys-sec/docs/tree/master/slides
  - No definition/problem questions on guest lectures
  - Guest lectures may be useful for essay, but not central
- Go through your notes
- If there is something unclear
  - Last opportunity to ask me
- Chocolates on the desk take some!

University of BRISTOL

Thank you, questions?

Office MVB 3.26

bristol.ac.uk