Sample Exam Questions (INSE 6150)

The following are questions from past exams for INSE 6150. The course content has changed a lot and so many questions are no longer relevant. I do not have an answer guide for the questions—they are provided as-is. You should study the notes, not these questions, as your exam will have new questions.

Question
A company produces an RFID card with a proprietary algorithm for performing encryption. Explain two methods for reverse-engineering the algorithm.

Question
Upon reverse-engineering, you discover the encryption function is secure but has a hardcoded key. Explain two methods for recovering the key.

Question
Explain step-by-step how to use return-oriented programming to execute malicious code on a vulnerable system.

Question
Alice logs into her banking website to pay a bill. Her browser offers to save her password for her. Assuming she allows it, name (a) one way this positively impacts usability, (b) one way it negatively impacts usability, (c) one way it positively impacts security, and (d) one way it weakens security. Make any reasonable assumptions your require to answer the question.

Question
If a certificate authority uses the applicant's website to validate ownership over a domain, describe three attacks on this process.

Question
Explain the difference between an extended validation certificate and a domain validated certificate for HTTPS in terms of (a) what they provide, (b) how they are issued, and (c) how users can tell them apart.

Question
Eve manages to successfully obtain a domain validated certificate for the domain `facebook.com\0.eve.com` where `\0` is a null symbol and `eve.com` is her actual domain. Explain how this might enable her to attack an internet user. State each assumption necessary for the attack and explain exactly what it enables her to do, provided the assumptions hold.

Question
Alice downloads a new app for her phone and instead of creating a new username and password for the app, she clicks the button "Log in with Facebook" which uses her

existing Facebook account to create a new account in the app. Name (a) one way this positively impacts security, (b) one way this weakens security, (c) one way this strengthens usability, and (d) one ways this weakens deployability. Make any reasonable assumptions your require to answer the question.

Question
Alice's company is developing a new online billing system. In order to ensure a good result, they first design the system on "paper" by developing a set of requirements and designing a specification of the system, and iterating until the specification matches the requirements. This is a good approach but misses one critical step: describe what it is.

Question
Alice works for a company that develops a web browser. To test for vulnerabilities, the company uses unit tests. Alice suggests using static analysis as well. List two advantages and two disadvantages of static analysis over unit tests.

Question
Does address space layout randomization mitigate buffer overflow attacks? If yes, explain how. If no, explain something that does prevent these attacks.

Question
Does control flow integrity mitigate return oriented programming? If yes, explain how. If no, explain something that does prevent these attacks.

Question
Does type safety prevent SQL injection attacks? If yes, explain how. If no, explain something that does prevent these attacks.

Question
Last year, Wikipedia enabled HTTPS by default on its website, primarily motivated by the possibility that nation-state's might eavesdrop on what articles were being looked at by its users. Is this a sufficient step to thwarting this attack? Why or why not?

Question
This exam was written on my personal laptop, printed over the network to a CIISE printer, photocopied in the CIISE copy room, and the stored in my locked office. Develop an attack tree for obtaining a copy of this exam prior to the exam date.

Question
In return oriented programming, what is a gadget? Your description should answer the following questions: where is the gadget located, who wrote it, and what is it used for?

Question
Mallory and Eve are both trying to attack a server with an internal IP address that they cannot access. Alice has access to the internal server. Both Eve and Mallory are able

to get Alice to click on a link to a website they control. Mallory hosts a website that embeds resources from the internal server inside an iFrame. Eve uses DNS rebinding to change the location of the resources from her website's IP address to the internal server's IP address. Are these two attacks equivalent in what they achieve? If so, justify your answer. If not, explain which is more powerful and why.

Question
Alice is asked by her employer to perform a cognitive walkthrough of a browser extension that allows users to see every cookie that is being set by each website the user visits. The user can block all cookies, allow all cookies. or choose to block individual cookies from a list. Identify and describe an appropriate set of core tasks for your walkthrough.

Question
An ATM is hardened against software attacks by placing all of its code on a read-only chip. The program counter is hardwired to only execute code on this chip. Is this sufficient to prevent arbitrary execution of malicious code? If yes, explain why it prevents known attacks? If no, explain how it could be defeated?

Question
A web application allows users to "like" products and displays how many likes each product has received. The number of likes is stored in an integer `count` initialized to zero (`count=0`). Upon clicking "like," the integer is increased by one (`count++`). No other methods in the code change the value of count. Mallory sees a product with 55 likes and wants to decrease it to 10. Given this specification of the code, is it sufficient to prevent this attack? Why or why not?

Question
Alice designs the following user study to test the usability of her new firewall software application. She posts an advertisement at a local grocery store and recruits 25 participants. She provides each participant with a written set of instructions for configuring a firewall. She measures the ease of which her subjects can (i) first configure an existing firewall application from a competitor and then (ii) configure her improved version. She learns that more participants succeed at configuring her firewall than the competitors', and in slightly less time as well!

Unfortunately, after releasing her software, Alice is surprised to learn that her users actually struggle with her firewall software—much more than they do with the competitors'. Explain the flaw(s) in her user study that contributed to her mistaken conclusion.

Question
You and Alice are hired by the university to audit the security surrounding final grades. Specifically, the university wants to know if you are able to access (with the ability to modify) the final grades for a particular course (in fine arts). The grades are stored in an Excel spreadsheet on the TA's computer in a lab on campus. He also stores a backup copy in Dropbox. Outline a social engineering attack with a good chance of

obtaining such access. In explaining your attack, emphasize the information gathering stage and any pretexting you might use (if used, the attack should be limited to two pretexts — one by you and one by Alice).

Question
(a) Name one advantage of static analysis over dynamic analysis. (b) Name one advantage of dynamic analysis over static analysis.

Question
Three attacks on software are code injection (CI), buffer overflows (BO), and return oriented programing (ROP). For each of the following mitigation techniques, list which of the three attacks it addresses (you can simply write down CI/BO/ROP; no additional marks for explanation): (a) Marking data as non-executable, (b) address space layout randomization, (c) taint analysis, (d) control flow integrity.

Question
In the Common Criteria, (a) the protection profile is used in which phase? What about (b) the evaluation assurance level?

Question
(a) Name one advantage of virtualization over sandboxing for containing software. (b) Name one advantage of sandboxing over virtualization.

Question
(a) Give an example of a cross-site scripting (XSS) attack. (b) Give an example of a cross-site request forgery (XSRF) attack. For both, clearly state what the attack allows the adversary to do, and what limitations the attack has.

Question
Alice signs up for two-factor authentication from Google. Now when she logs into her gmail account, she receives a text message on her phone with a one-time code that she types in along with her password to log-in. Name (a) one way it positively impacts security, (b) one way it weakens security, (c) one way it weakens usability, and (d) one ways it weakens deployability. Make any reasonable assumptions your require to answer the question.

Question
(a) What is an air-gap and why is it used? (b) Give an example of how an adversary could defeat an air-gap.

Question
(a) State the STRIDE threat category of an amplification attack. (b) Describe how the attack works. (c) Name a common webservice that could enable the attack (or has in the past).

Question
(a) Explain how a trusted platform module (TPM) provides a secure boot. (b) What security properties does a secure boot provide and (c) what are its limitations?

Question
(a) What is the same origin policy (SOP) used for by browsers? Consider my website at http://users.encs.concordia.ca/~clark/. (b) Write a URL that is considered the same origin. (c) Write a URL, within concordia.ca, that is not the same origin.

Question
Recall secure function evaluation (SFE) enables the secure computation of a program. (a) State and define the two security properties a SFE can provide. (b) State what it means for a SFE to be in the "honest-but-curious" model.

Question
Recall that there are four categories of SFE: verifiable computing (VC), two-party computation (2PC), multi-party computation (MPC), and homomorphic encryption (HE). For each scenario below, state which of the four is the most appropriate with one or two sentences of explanation:
(a) Alice conducts a live auction of her artwork online with many bidders. Alice should be able to determine the winning bid but all other bids should remain secret;
(b) Alice and Bob want to determine who is richer without revealing their worth;
(c) Dr. Alice is on her smartphone and needs the result of an intensive genetic test done on a set of genomes stored by an unreliable cloud;
(d) Alice conducts an election with many voters casting their ballots over several days. Alice should be able to determine the winner but not who voted for whom.

Question
A company produces an RFID chip with a proprietary algorithm for performing encryption. (a) Explain two methods for reverse-engineering the algorithm. Upon reverse-engineering, you discover the encryption function is secure but has a hardcoded key. (b) Explain two methods for recovering the key.

Question
(a) Explain what attacks the meta-compilation methodology addresses. (b) Give an example of a global extension and a variable-specific extension. (c) What is a basic block and what is recorded in a block summary?

Question
A company produces a new cryptographic authentication protocol and provides a security proof. The security proof is a game-based proof. (a) Name one limitation this protocol *will have* (not "might have") given its security proof. (b) Explain what the "ideal world" is in a simulation-based proof and how it assists the security proof.

Question

Explain each of the four phases of requirements engineering, using one or two sentences per phase.

Question
A user has the following cookies set in her browser:

`(C1) Set at https://www.dictionary.com/browse/automata, no scope specified.`

`(C2) Set at https://www.dictionary.com/browse/automata, marked secure, scope specified as *.dictionary.com.`

`(C3) Set at https://images.secure-ads.com/index.html, marked secure, marked https-only, scope specified as *.images.secure-ads.com.`

A user navigates to `https://www.dictionary.com/` which makes a number of calls to other web resources (`*.jpg` are images and `*.js` is javascript) to construct the page:

(1) `GET https://www.dictionary.com/browse/abacus`
(2) `GET https://images.dictionary.ca/logo.jpg`
(3) `GET https://scripts.dictionary.com/newaccount.js`
(4) `GET http://www.facebook.com/like.js`
(5) `GET https://www.secure-ads.com/get_ad.js`

The `get_ad.js` script then loads the following image:

(6) `https://images.secure-ads.com/ad-0139.jpg`

Answer the following questions about these requests:

(a) List which cookie is sent for each request:

Request:	1	2	3	4	5	6
Cookie(s):						

(b) Is the site displayed with an HTTPS lock? Why or why not?

Question

A user has the following two cookies set in her browser:

```
(C1) Set at https://www.concordia.ca/index.html, marked
secure, no scope specified.

(C2) Set at https://images.secure-ads.com/index.html,
marked secure, scope specified as *.images.secure-ads.com.
```

A user navigates to `https://www.concordia.ca/students.html` which makes a number of calls to other web resources (`*.jpg` are images and `*.js` is javascript) to construct the page:

```
(1) GET https://www.concordia.ca/students.html
(2) GET https://images.concordia.ca/logo.jpg
(3) GET https://www.secure-ads.com/get_ad.js
(4) GET https://images.secure-ads.com/ad-0139.jpg
```

The student then follows a link to check her marks, which makes the following web requests:

```
(5) GET https://www.concordia.ca/grades.html
(6) GET http://www.concordia.ca/get_grades.js
(7) GET https://www.secure-ads.com/get_ad.js
(8) GET https://images.secure-ads.com/ad-9872.jpg
```

Answer the following questions about these requests:

(a) For which flow(s) (1-8) is an HTTPS warning/error generated and why?
(b) For which flow(s) (1-8) is Cookie 1 sent and why?
(c) For which flow(s) (1-8) is Cookie 2 sent and why?

Question

For each of the following scenarios, circle the **one** STRIDE threat category it fits best into. You may circle the same category more than once.

Mallory looks through a company's outdoor garbage bins and finds financial records.					
S	T	R	I	D	E
Mallory enters a business and talks to an office administrator while impersonating an IT contractor.					
S	T	R	I	D	E
Mallory breaks an RFID reader on a locked door she does not have access to.					
S	T	R	I	D	E
Later, Mallory returns to find that the door is being held ajar by a book so employees can enter. She walks in.					
S	T	R	I	D	E
Mallory installs malware on the CEO's computer.					
S	T	R	I	D	E
Later after Mallory is caught, the office administrator denies ever talking to Mallory.					
S	T	R	I	D	E

Question

Recall that the STRIDE methodology for determining threats is an acronym for six threat categories. For each of the following scenarios, state which threat category it fits best into (no explanation necessary):

(a) Mallory uses a botnet to flood an internet voting server during an election;
(b) Mallory exploits a loophole in airport security procedures to board a flight despite being on the no-fly list;
(c) Mallory conducts a XSS attack;
(d) Mallory conducts a XSRF attack;
(e) Mallory uses Heartbleed to steal Alice's authentication cookie;
(f) Mallory examines the packet length of an encrypted flow to determine what websites Alice is visiting;
(g) Mallory buys a new computer with her credit card, and then tells her bank that her card was stolen and she didn't make the purchase.

Question
Consider the following pseudocode:

```
string MD5(string m){
  string output;
  output = …omitted…;
  return output;
}
```

```
string SHA256(string m){
  string output;
  output = …omitted…;
  return output;
}
```

```
string cert(string m){
  cert1=sign(m,MD5);
  cert2=sign(m,SHA256);
  return cert2;
}
```

The functionality of the code is not relevant to the question. Briefly, two hash functions, `MD5()` and `SHA256()`, are defined. These functions are called by the subfunction `sign()` of a function `cert()`. Assume that the pointer to the hash function in `sign()` is stored in register `R`. To prevent certain attacks, Alice instruments her code with flow integrity. Part of this is already shown below. Complete the parts marked [_____] by filling in the appropriate labels or by leaving them empty.

```
MD5( )
  label “ABC”
  …
  return “NTE”
```

```
SHA256( )
  [_____]
  …
  return [_____]
```

```
cert( )
  label “XSD”
  …
  call sign [_____]
  label “DUW”
  …
  call sign [_____]
  [_____]
  …
  return “EGE”
```

```
sign( )
  label “XRI”
  …
  call R [_____]
  [_____]
  …
  return [_____]
```