**Quiz 01**

1. Imagine you are analyzing the usability of a banking website. Which of the following are examples of good tasks?

* How many types of accounts are available?
* Transfer $20 from checking to savings.
* Open a new savings account.
* Go to the banking login screen. Enter your username and password. Once your account list appears, click on your checking account. Then read the third item in the list of transactions.
* Check your savings account balance.
* Search for a deposit transaction.

**Answer**

* Transfer $20 from checking to savings.
* Open a new savings account.
* Check your savings account balance.

**Question 02**

Which of the following are measures of usability?

* Speed
* User Preference
* Efficiency
* Design uniqueness
* Learnability
* Memorability
* Codability

**Answer**

* Speed
* User Preference
* Efficiency
* Learnability
* Memorability

**Question 03**

What is chunking?

* Repeating information over and over to help memorize it.
* Aggregating several pieces of information into coherent groups to make them easier to remember.
* Breaking a long list of pieces of information into smaller groups.

**Answer**

* Aggregating several pieces of information into coherent groups to make them easier to remember.

**Question 04**

Which of the following are examples of conventions that improve mental models?

* Putting options to create a new file and save a file under a "File" menu in the upper left of the application.
* Making all controls for an interface visible.
* Providing feedback on user actions.
* Using a qwerty keyboard on a new device.
* Color coding warnings in red and alerts in yellow.

**Answer**

* Putting options to create a new file and save a file under a "File" menu in the upper left of the application.
* Using a qwerty keyboard on a new device.
* Color coding warnings in red and alerts in yellow.

**Question 05**

Human-Computer Interaction is the study of:

* The artwork created by people using computers.
* How people interact with technology.
* How computers take jobs away from people.

**Answer**

* How people interact with technology.

**Question 06**

The people included in an HCI study might include:

* Desktop or Laptop Computer Users.
* Mobile Device Users.
* Users who have Technology Embedded in Wearable Items.
* All of the above.

**Answer**

* All of the above.

**Question 07**

Three important things that have to be understood in HCI are:

* Users, Tasks, and Context.
* Location, Age and Education.
* Screen Sizes, Processor Speeds and Memory Sizes.

**Answer**

* Users, Tasks, and Context.

**Question 08**

How should users be considered within a security system?

* They need to be well-trained in how to use the security systems we build for them.
* They are often the reason security fails.
* They are an integral part of security and should be considered part of the system from the beginning.

**Answer**

* They are an integral part of security and should be considered part of the system from the beginning.

**Question 09**

HCI is based on an understanding of human's cognitive abilities.

* True
* False

**Answer**

* True

**Question 10**

Which of the following are factors to consider in designing usable interfaces?

* The users' expertise and experience with computers.
* The impact the interface will have on the cost of the system.
* The efficiency of the code that runs the system.

**Answer**

* The users' expertise and experience with computers.

Quiz 2.

Вопрос 1

1. What is the cycle of the iterative design process?

Requirements - Design - Development – Testing

2. What's the difference between system centered design and user centered design

System centered design is focused on what is easy to build on a platform while user centered design is focused on user needs and context.

3. Which of the following are NOT good ways to incorporate user-centered design in the design of security systems?

Designing security based on what experts believe is best.

4. When designing error messages, which are important factors to keep in mind for usability?

Provide users with clear exits to get out of a security warning

Make the most secure options part of the user's natural task

5. If you were designing security for the entrance to a secure facility, which of the following should you consider?

How often users enter and exit

What tasks the users are in the middle of when they need to access the area.

6. Which of the following are disadvantages of personas?

A diverse audience may be difficult to represent with a normal-sized set of personas

Too many personas can be difficult to create and manage.

7. Which of these are advantages of low-fidelity (e.g. paper) prototypes

They can be created quickly and cheaply

Any team member can create one, regardless of programming skills

8. Which of the following are present in good interface design?

Minimal training needed for a person to use the system

Relies on common interaction techniques for familiarity

Easy to recover from errors

9. Which of the following is NOT an important part of the design process

Compute the efficiency of the underlying algorithms

10. In participatory design and co-design, which of the following is true

Average users have equal standing with designers.

Quiz 3.

1. What is the goal of A/B testing?

To compare the performance two (or more) interface variations

2. What is a heuristic evaluation?

Analyzing a system according to a set of guidelines for good usability.

3. What is the goal of a usability study?

To measure and describe usability of a system for given tasks

4. If we ran an experiment to test if password logins were faster than a voice recognition authentication system, what would be required to show passwords were faster?

Statistical tests showed that the password group logged in significantly faster than the voice-recognition group.

5. Which of the following is not something you would do when running a controlled experiment to evaluate an interface?

Select average users to test the control interface and expert users to test the experimental interface.

6. Qualitative evaluation is intended to:

Understand user experiences and reactions to a design

7. Which of the following is NOT a standard observation method

Assisted Use

8. Why do we conduct usability studies on systems that have already been designed?

Despite their best efforts, designer and developers cannot know exactly how users will interact with their system. A usability study will find previously uncovered errors.

9. Which of the following are typical questions to ask on a pre-test questionnaire?

What is your highest level of education

What is your age

10. When conducting a controlled experiment, which of the following is not part of the process

Explain to participants what conclusions you hope to draw from the results.

Quiz 4.

1. What is the principle of least privilege?

A system should be able to access only the information it needs to perform its functions

2. Which of the following is not a guideline for creating usable security systems?

Prevent users from granting authority unless their request is approved by the security staff

3. Which of the following is a good guideline about showing detail to users?

Show a level of detail that’s informative and useful to the user, and no more than that

4. If you are warning users about a security problem that has been detected, which is the best message to show them?

A message that alerts them to the error and makes the most obvious option the one that stops the user from proceeding. A small link is given to ignore the warning and proceed.

5. In a system where a person can grant authority to others to his or her own access resources, which of the following is true?

The interface should help users be aware of what authority they have granted in the past

The easiest way to do a task should require the most minimal granting of authority

Users should be able to reduce the authority granted to others.

6. True or False: A design guideline for creating usable secure systems is to make the most secure way to complete a task the easiest way to complete the task

True

7. For an average user, which of the following is the most usable way to set file permissions?

A pop up menu that allows a user to select a document as "private", "shared with select users", or "public". If one of the latter two options are selected, the user is then prompted to select "others can read" or "others can edit"

8. Which guideline is violated when an interface does not make capitalization differences unambiguous (e.g. a lower case "L" and capital "i" appear to be the same thing).

Make it easy to see the differences between objects and actions that could be confused.

9. True or false: Users should be aware of what authority they hold, what authority they have granted, and what the implications are for security decisions

True

10. Which of the following is true?

The more usable a system is, the less secure it is because users do not understand security, so to make a usable system, security must be downgraded or left off.

(True) The more usable a system is, the more secure it is because usable systems help users make good security decisions and easily choose the most secure actions

Quiz 5.

1. What type of attack would be most effective / fastest if the user's password is "hello"?

Common Word

2. Which of the following passwords is most secure?

sometimes extra student clever

3. True or False: Two factor authentication improves the security and usability of a system.

False.

4. Which of the following is not a type of biometric authentication?

PIN code

5. Which of the following is NOT a method for obtaining a second factor authentication code?

Choosing a memorable year in one's life

6. Which of the following is not a type of gesture based authentication?

Typing in a numeric code on a keypad

7. In the paper on smudge attacks, on which phone was it easiest to find password information?

Phone that touched the face

8. Which of the following improves security of a traditional password system?

Limitations on the number of incorrect logins in a fixed time frame

9. True or false: fingerprint recognition is generally faster than password entry for authentication.

True

10. Which of the following are measures of usability for authentication systems?

Speed

Likelihood of error

How easy it is to learn.

Quiz 6.

1. Which of these is not a guideline for usable privacy?

Provide detailed privacy controls

2. A mobile app uses a phone's microphone to listen in the background for commercials, songs, and TV shows that a person is hearing in order to target ads at the user. The app does not store any information about users' conversations nor does it store recordings. Should the app disclose that it is listening to this background sound?

Yes, users should be informed that sound from their environment is being collected.

3. Which of the following is true of privacy policies?

When people read them, they often feel like they don't understand them.

4. True or false: Alternatives to privacy policies can be as effective in teaching users about how their data is shared.

True

5. Which of these attributes can be automatically inferred on social media, even if users don't provide any obvious clues.

All of the Above

6. If a company has collected an American user's personal data without their consent, how can the user respond?

They have no rights to their data.

7. Which of the following describes informed consent?

A person knows how their data is used and competently agrees to that use.

8. A website provides an extensive 50-printed-page privacy policy written in common language that describes every detail of how users' data is collected, used, and shared. Which of the following is true of informed consent?

The policy does not meet the requirement of minimal distraction

9. Which of the following questions is NOT answered as part of the disclosure component of informed consent?

What privacy settings do users have access to?

10. True or false: Providing complete and detailed explanations of how data is collected and used can overwhelm the user and lead to a less usable privacy system.

True.

Quiz 7.

1. Company ABC's password policy has always been that the system generates passwords for its users instead of letting them pick their own. The passwords are random 8-character strings with upper and lower case letters, numbers, and symbols for users (e.g. "^8j4Z.mp"). Every six months, the password is changed to something new. Because password resets are a security danger, users are not allowed to reset their passwords if they forget them. Instead, they need to go to the company's IT office which looks up their existing password and gives them a printout with the password on it.

(note: this is a true example – I worked at an organization that had exactly this policy)

Answer the questions 1-13 about Company ABC's policy.

True or false: the passwords that the system generate are very hard to crack?

True.

2. Which method would work best if trying to crack one of Company ABC's passwords

Brute force.

3. What is the biggest usability problem with Company ABC's passwords?

They are hard to remember (memorability)

4. Which of the following is the most likely response to Company ABC's password reset policy?

Users will write down their passwords.

5. True or false: a policy that allows users reset their passwords automatically (e.g. if a user forgets their password they can enter their user ID and have a new password emailed to the address that the IT office has on file) may lead users choosing more complex passwords.

True.

6. True or false: a policy that users reset their passwords automatically would be more usable

True.

7. True or false: a user-chosen 8-character password would be more difficult to break than the existing system-generated passwords.

False.

8. True or false: a user-chosen 8-character password would be more usable.

True.

9. True or false: a user chosen 8-character password could be more secure.

True.

10. True or false: an automatically generated password that combined 4 unrelated common words would be harder to break.

True.

11. True or false: an automatically generated password that combined 4 unrelated common words would be more usable.

True.

12. True or false: Increasing the usability of Company ABC's password policy would lead to greater security.

True.

13. True or false: There is a conflict between creating a usable password system and the most secure password system

False.

14. Company XYZ is a defense contractor. They need to make sure that only authorized people enter their facilities. They have decided to install a new biometric authentication station outside the gate that protects the parking lot. Employees will need to authenticate in order to be let in. Answer questions 14-20 about Company XYZ.

How should the security system be designed?

The designer should sit at the gate during the busiest time of morning and evening and watch people come in and out.

15. If someone tries to authenticate and they are not recognized, the system designer is considering adding a delay before they can try to authenticate again. Which is the best delay?

10 seconds.

16. A survey shows that a surprisingly large percentage (25%) of employees ride motorcycles to work, the standard protective gear of helmets, leather jackets, and gloves. Which of the following would be a poor biometric tool based on this fact?

Face recognition.

17. The designer has decided to use a free gesture system to authenticate people, but the hardware for a gesture-detection system that is weatherproof is very expensive. As she is eating lunch in her office, she is contemplating the next step. What should she do?

Her lunch's pizza box is about the size of the gesture reading hardware. She should paint the box and position it at the gate where the real tool would go, and then ask people to pretend to authenticate as they come in so she can get information about the process. If people don't like it, she can revise the design

18. The free gesture system is implemented, and all employees have stopped by the IT office to teach the system what their authenticating gesture is by entering it on a touch screen in the office. A couple weeks later, people who drive SUVs start complaining that they sometimes need to enter their gesture 4 or 5 times because it is not recognized (probably because they are making it from an odd angle – their cars are high up above the device where they enter their gesture). What type of usability problem is this?

Efficiency.

19. What is a good solution for the SUV drivers?

When they teach the system what their authenticating gesture is, they should do it from their car rather than in the IT office so there is a better match between their "true" gesture and what they enter when they drive in

20. After a while, the IT office complains to the designer that people keep coming in having forgotten their gestures. This is a problem because traffic backs up when a person can't remember the gesture, it takes a lot of time to reset the gesture, and people are trying to get around the system by closely following the person in front of them through the open gate. The designer decides that from now on, when people create new gestures, it should be the person's normal signature. Which usability aspect does this improve?

Memorability.

21. Answer questions 21-24 about Company 123.

Company 123 is creating a social network designed to compete with Facebook. They begin by copying Facebook's interface exactly, except they change the name and make it green instead of blue. How does this help usability?

It lets users rely on existing mental models

22. Company 123 writes a privacy policy that is written in easy-to-read language at an 6th grade reading level and is exactly 1 page long when printed and that covers all the major points of their privacy – mainly, that no data is ever shared except with people the user lists in their own privacy settings. Which of these five pitfalls does their policy avoid:

Obscuring actual information flow.

Obscuring potential information flow.

23. Is a 12-year old in 7th grade able to give informed consent to this policy?

No.

24. A designer at Company 123 is considering changing their login interface so the password box shows the last character typed for 1 second before changing it to the standard star or dot that prevents over the shoulder attacks. They hope this will help people spot when they have made a typo as they enter their password. How should she determine if this is a good change to make?

Run an A/B test and see which version has fewer failed logins.

25. True or false: error messages should limit technical detail in favor of plain language.

True.

Part 2.

Quiz 1.

1. This test is meant to test your knowledge of C programming and some basic computer science-related skills you will need to do well in this class. The outcome of the test is for your use only; it will not affect whether you can register for the class, and it will not apply to your grade if you do register. As such, we recommend that you do not research the answers on the Internet, but answer the questions to your best recollection.

Consider the following variable declaration for

bar

bar in the function

foo

foo

Holds 128 elements.

2. Consider the following code fragment:

sizeof(int\*) == sizeof(int)

sizeof(int\*) == sizeof(int). Which one of the following is true about it?

This fragment's result depends on the compiler and architecture.

3. Suppose you are compiling for a 32-bit platform and sizeof(int) == 4. Which one of the following is equivalent to c[b] if c is of type int\* and b is of type int?

\*(c+b)

4. Consider the following program.

#include <string.h>

int foo(void) {

char bar[128];

char \*baz = &bar[0];

baz[127] = 0;

return strlen(baz);

}

Returns 127.

5. Consider the following code fragment

char blah[] = "fizzbuzz";

printf("%s\n", blah+4);

The program outputs "buzz".

6. Which of the following are true of memory returned via the malloc function? Check all that apply.

It must be manually released by the programmer.

7. Consider the following code.

#include <stdio.h>

#include <stdlib.h>

int main(int argc, char \*argv[]) {

unsigned int i;

unsigned int k = atoi(argv[1]);

char \*buf = malloc(k); /\* 1 \*/

if(buf == 0) {

return -1;

}

for(i = 0; i < k; i++) {

buf[i] = argv[2][i]; /\* 2 \*/

}

printf("%s\n", buf); /\* 3 \*/

return -1;

}

This program could crash at 2 and 3.

8. Which of the following are true statements about the program stack?

It is used to store local variables while executing a function

The stack is managed by code emitted by the compiler.

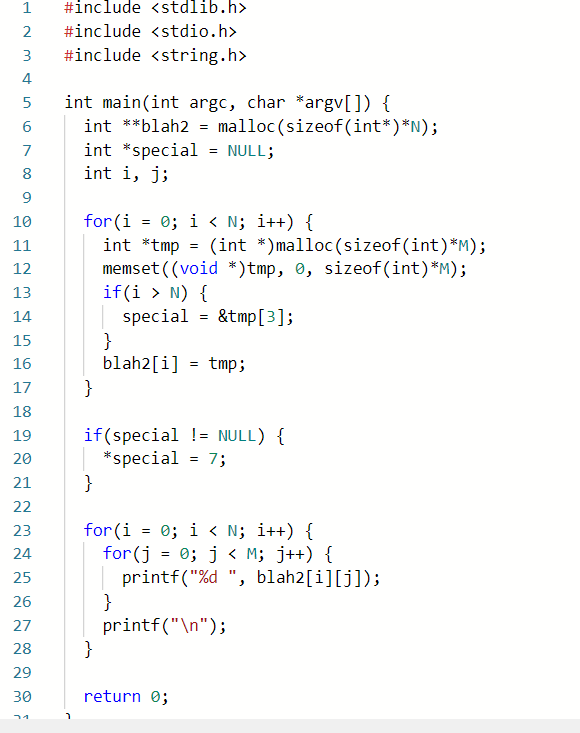
9. Which of the following are true of the X86 call instruction?

Branches to a specified address

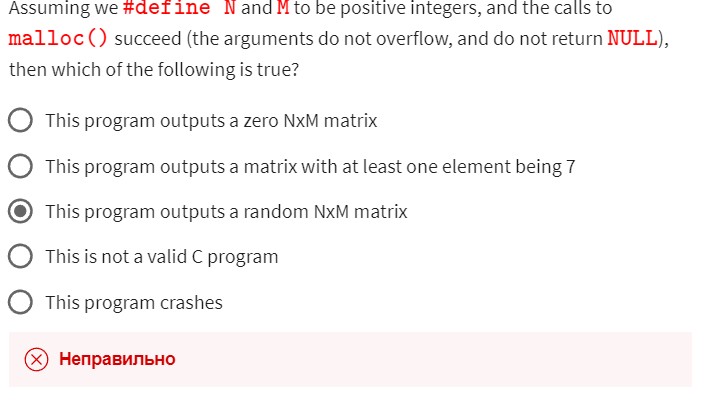
Pushes the instruction pointer value onto the stack

Its target address may be specified in a general-purpose register.

10. Consider the following program.



Assuming we #define N and M to be positive integers, and the calls to malloc() succeed (the arguments do not overflow, and do not return NULL), then which of the following is true?



11. What is TCP?

It is a protocol that supports reliable data transfer on the Internet.

12. What is PHP? Pick one.

A programming language often used to implement web sites.

13. Which of the following statements about HTML are true?

HTML is a text-based format (as opposed to a binary format)

Web browsers render HTML content served by web sites

HTML documents have tags that identify different sorts of data.

14. What is gcc?

A compiler.

15. The shell command cd; ls \*.xml

Will list all files ending in the xml suffix in user's home directory.

Quiz 2.

1. Three of the following are classic security properties; which one is not?

Availability

Confidentiality

Correctness (+)

Integrity

2. What was the first buffer overflow attack?

Love Bug

SQL Slammer

Morris Worm (+)

Code Red

3. The stack is memory for storing

Local variables (+)

Program code

Dynamically linked libraries

Global variables

4. Why is it that the compiler does not know the absolute address of a local variable?

Programs are not allowed to reference memory using absolute addresses

The size of the address depends on the architecture the program will run on

As a stack-allocated variable, it could have different addresses depending on when its containing function is called (+)

Compiler writers are not very good at that sort of thing

5. When does a buffer overflow occur, generally speaking?

when writing to a pointer that has been freed

when copying a buffer from the stack to the heap

when a pointer is used to access memory not allocated to it (+)

when the program notices a buffer has filled up, and so starts to reject requests

6. How does a buffer overflow on the stack facilitate running attacker-injected code?

By overwriting the return address to point to the location of that code (+)

By writing directly to the instruction pointer register the address of the code

By writing directly to %eax the address of the code

By changing the name of the running executable, stored on the stack

7. What is a nop sled?

It is an anonymous version of a mop sled

It is a sequence of nops preceding injected shellcode, useful when the return address is unknown (+)

It is a method of removing zero bytes from shellcode

It is another name for a branch instruction at the end of sequence of nops

8. The following program is vulnerable to a buffer overflow (assuming the absence of automated defenses like ASLR, DEP, etc., which we introduce in the next unit). What is the name of the buffer that can be overflowed?

#include <stdio.h>

#include <string.h>

#define S 100

#define N 1000

int main(int argc, char \*argv[]) {

char out[S];

char buf[N];

char msg[] = "Welcome to the argument echoing program\n";

int len = 0;

buf[0] = '\0';

printf(msg);

while (argc) {

sprintf(out, "argument %d is %s\n", argc-1, argv[argc-1]);

argc--;

strncat(buf,out,sizeof(buf)-len-1);

len = strlen(buf);

}

printf("%s",buf);

return 0;

}

out (+)

len

buf

msg

9. Here is the same program as the previous question. What line of code can overflow the vulnerable buffer?

#include <stdio.h>

#include <string.h>

#define S 100

#define N 1000

int main(int argc, char \*argv[]) {

char out[S];

char buf[N];

char msg[] = "Welcome to the argument echoing program\n";

int len = 0;

buf[0] = '\0';

printf(msg);

while (argc) {

sprintf(out, "argument %d is %s\n", argc-1, argv[argc-1]);

argc--;

strncat(buf,out,sizeof(buf)-len-1);

len = strlen(buf);

}

printf("%s",buf);

return 0;

}

sprintf(out, "argument %d is %s\n", argc-1, argv[argc-1]); (+)

printf(msg)

len = strlen(buf);

strncat(buf,out,sizeof(buf)-len-1);

printf("%s",buf);

10. Recall the vulnerable overflow from the previous two questions. We can change one line of code and make the buffer overrun go away. Which of the following one-line changes, on its own, will eliminate the vulnerability?

#include <stdio.h>

#include <string.h>

#define S 100

#define N 1000

int main(int argc,char \*argv[]) {

char out[S];

char buf[N];

char msg[] = "Welcome to the argument echoing program\n";

int len = 0;

buf[0] = '\0';

printf(msg);

while (argc) {

sprintf(out,"argument %d is %s\n",argc-1,argv[argc-1]);

argc--;

strncat(buf,out,sizeof(buf)-len-1);

len = strlen(buf);

}

printf("%s",buf);

return 0;

}

change printf("%s",buf) to printf(buf);

change printf(msg) to printf("%s",msg);

change char msg[] = "Welcome to the argument echoing program\n" to char msg[42] = "Welcome to the argument echoing program\n"

change sprintf(out, "argument %d is %s\n", argc-1, argv[argc-1]) (+)

to snprintf(out, S, "argument %d is %s\n", argc-1, argv[argc-1])

11. Recall the vulnerable program from the previous few questions. Which of the following attacks do you think the program is susceptible to?

#include <stdio.h>

#include <string.h>

#define S 100

#define N 1000

int main(int argc, char \*argv[]) {

char out[S];

char buf[N];

char msg[] = "Welcome to the argument echoing program\n";

int len = 0;

buf[0] = '\0';

printf(msg);

while (argc) {

sprintf(out, "argument %d is %s\n", argc-1, argv[argc-1]);

argc--;

strncat(buf,out,sizeof(buf)-len-1);

len = strlen(buf);

}

printf("%s",buf);

return 0;

}

code injection

data corruption

reading arbitrary addresses in memory

all of the above (+)

12. Recall the program again.

#include <stdio.h>

#include <string.h>

#define S 100

#define N 1000

int main(int argc, char \*argv[]) {

char out[S];

char buf[N];

char msg[] = "Welcome to the argument echoing program\n";

int len = 0;

buf[0] = '\0';

printf(msg);

while (argc) {

sprintf(out, "argument %d is %s\n", argc-1, argv[argc-1]);

argc--;

strncat(buf,out,sizeof(buf)-len-1);

len = strlen(buf);

}

printf("%s",buf);

return 0;

}

If we changed printf("%s",buf) to printf(buf) then the program would be vulnerable to what sort of attack?

heap overflow

format string attack (+)

use-after-free attack

all of the above

13. Exploitation of the Heartbleed bug permits

overwriting cryptographic keys in memory

a kind of code injection

a read outside bounds of a buffer (+)

a format string attack

14. Why is it that anti-virus scanners would not have found an exploitation of Heartbleed?

It's a vacuous question: Heartbleed only reads outside a buffer, so

there is no possible exploit

Anti-virus scanners tend to look for viruses and other malicious

code, but Heartbleed exploits steal secrets without injecting any code (+)

Heartbleed exploits are easily mutated so the files they leave

behind do not appear unusual

Heartbleed attacks the anti-virus scanner itself

15. An integer overflow occurs when

an integer expression's result "wraps around"; instead of creating a very large number, a very small (or negative) number ends up getting created (+)

an integer is used as if it was a pointer

an integer is used to access a buffer outside of the buffer's bounds

there is no more space to hold integers in the program

Quiz 3.

1. There is a stack-based overflow in the program.

What is the name of the stack-allocated variable that contains

the overflowed buffer?

ans: wis

2. Consider the buffer you just identified:

Running what line of code will overflow the buffer?

ans: 62

3. There is another vulnerability, not dependent at all on the first,

involving a non-stack allocated buffer that can be indexed outside

its bounds. What variable contains this buffer?

ans: ptrs

4. Consider the buffer you just identified: Running what line of code overflows the buffer?

ans: 101

5. What is the address of buf?

ans: 0xbffff130

6. What is the address of ptrs?

ans: 0x0804a0d4

7, What is the address of write\_secret?

ans: 0x08048534

8. what is the address of p local to main?

ans: 0xbffff534

9. What input do you provide so that ptrs[s] reads/executes

the contents of variable p instead of function in ptrs buffer?

If ok, you will execute pat\_on\_back function. Enter your answer

as an unsigned integer.

ans:

(p-ptrs)/4 is

print /x (0xbffff534 - 0x804a0d4)/4

0x2dfed518 or **771675416**

10. What do you enter so that ptrs[s] reads (and then tries to execute)

starting from the 65th byte in buf, ie. the location at buf[64]?

Enter your answer as an unsiged integer.

ans:

(gdb) print /x &buf[64]

$6 = 0xbffff170

(gdb) print /d (int\*)&buf[64]-(int \*)&ptrs

$14 = 771675175

**771675175**

11. What do you replace \xEE\xEE\xEE\xEE with to call write\_secret?

ans:

(gdb) print &write\_secret

$7 = (void (\*)(void)) 0x8048534 <write\_secret>

**\color{red}{\verb|771675175\x00AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA\x34\x85\x04\x08|}**

12. Suppose you wanted to overflow the wis variable to perform a stack smashing attack. You could do this by entering 2 to call put\_wisdom, and then enter enough bytes to overwrite the return address of that function, replacing it with the address of write\_secret. How many bytes do you need to enter prior to the address of write\_secret?

148

Quiz 4.

1. A program indexes a buffer after a pointer to that buffer has been used as a parameter to the free() function. This is

**A violation of temporal memory safety**

Correct behavior

A violation of spatial memory safety

An information flow violation

2. When could an integer overflow impact memory safety?

If the integer was passed as a parameter to open()

**If the integer is passed as an argument to malloc()**

If the integer was passed as a parameter to printf()

**If the integer was used to perform pointer arithmetic**

If the integer is used as the denominator in a division expression

3. Which of the following are true about a language that uses garbage collection or some other automatic means (e.g., reference counting) for memory management? (Select all that apply.)

**The language will not have spatial memory safety violations**

**The use of automatic memory management will provide a safety benefit, but typically at the cost of some performance**

The language will not have type safety violations

4. Consider the following code:

char \*foo(char \*buf) {

char \*x = buf+strlen(buf);

char \*y = buf;

while (y != x) {

if (\*y == 'a')break;

y++;

}

return y;

}

void bar() {

char input[10] = "leonard";

foo(input);

}

The definition of spatial safety models pointers as capabilities, which are triples (p,b,e) where p is the pointer, b is the base of the memory region the pointer is allowed to access, and e is the extent of that region. Assuming characters are 1 byte in size, what is a triple (p,b,e) for the variable y when it is returned at the end of the code?

(y,&input,buf)

(&input+4,&input,&input+7)

**(&input+4,&input,&input+10)**

(&input+4,0,sizeof(input))

5. Which of the following are true about a type-safe language? (Select all that apply.)

The language is object-oriented.

The language is always much slower than a non-type safe language

The language is also memory safe

**The language is sometimes memory safe, but not always**

6. An engineer proposes that in addition to making the stack non-executable, your system should also make the heap non-executable. Doing so would

**Make the program more secure by disallowing another location for an attacker to place executable code**

Not make the program more secure, because attacker-controlled data cannot be stored in the heap

Ensure that only the correct amount of data was written to a heap-allocated block, preventing heap overflows

Ensure that memory is always deallocated

7. What is the best choice of value for a stack canary, of the following options?

The constant 0

The constant 7

A predictable value

**A random value**

8. A return-to-libc attack does not require that the attacker inject executable code into the vulnerable program. Which of the following is the most important reason that return-to-libc attacks are useful to the attacker?

**There is no need to be able to execute (writable) data**

The injected code might have bugs

The code in libc is better than code the attacker would write

There is no need to modify the application's executable code

9. In a return-oriented program (ROP), what is the role of the stack pointer?

It's like the frame pointer in a normal program

It's really no different than in a normal program

It's like the allocation pointer used by malloc()

**It's like the program counter in a normal program**

10. When enforcing Control Flow Integrity (CFI), there is no need to check that direct calls adhere to the control flow graph because:

**CFI should be deployed on systems that ensure the data is non-executable**

Programs that use CFI don't have direct calls

The attacker is not interested in corrupting direct calls

CFI should be deployed on systems that ensure the code is immutable

11. Recall that classic enforcement of CFI requires adding labels prior to branch targets, and adding code prior to the branch that checks the label to see if it's the one that is expected. Now consider the following program:

int cmp1(char \*a, char \*b) {

return strcmp(a,b);

}

int cmp2(char \*a, char \*b) {

return strcmp(b,a);

}

typedef int (\*cmpp)(char\*,char\*);

int bar(char \*buf) {

cmpp p;

char tmpbuff[512] = { 0 };

int l;

if(buf[0] == 'a') {

p = cmp1;

} else {

p = cmp2;

}

printf("%p\n", p);

strcpy(tmpbuff, buf);

for(l = 0; l < sizeof(tmpbuff); l++) {

if(tmpbuff[l] == 0) {

break;

} else {

if(tmpbuff[l] > 97) {

tmpbuff[l] -= 32;

}

}

}

return p(tmpbuff,buf);

}

To ensure that the instrumented program runs correctly when not being attacked, which of the following functions would have to be given the same label? Choose at least two, but no more functions than necessary.

strcpy

**cmp1**

**cmp2**

cmpp

strcmp

12. In your review of a program, you discover the following function:

void aFunction(char \*buf) {

static char BANNED\_CHARACTERS[] = { '>', '<', '!', '\*' };

int l = strlen(buf);

int i;

for(i = 0; i < l; i++) {

int j;

int k = sizeof(BANNED\_CHARACTERS) / sizeof(char);

for(j = 0; j < k; j++) {

if(buf[i] == BANNED\_CHARACTERS[j])

buf[i] = ' ';

}

}

}

How would you best describe what this function is doing?

Input validation by whitelisting

**Input sanitization by blacklisting**

Spatial safety enforcement

Using a safe string library

13. A safe string library typically attempts to ensure which of the following?

**That there is sufficient space in a source and/or target string to perform operations like concatenation, copying, etc.**

That the strings have been properly sanitized

That wide (i.e., multibyte) character strings can be used where single-byte character strings are expected.

That strings from the safe library can be freely passed to the standard string library functions, and vice versa

14. A project manager proposes a C coding standard where pointer variables must be assigned to NULL after being passed to free(). Doing so:

Helps code readability, but not security

Is a poor security decision, because NULL pointer dereferences could cause the program to crash

**Stops writes to stale pointer values that might otherwise succeed and result in program compromise**

Prevents memory leaks, thus avoiding potential denial of service

15. A colleague proposes using a heap allocator that randomizes the addresses of allocated objects. This:

Will increase performance by keeping the cache sparsely populated

**Will make the program more secure, because attackers frequently rely on predicting the locations of heap-allocated objects in exploits**

Will make the program less secure, because the application will not be able to predict the locations of heap-allocated objects

Will have no impact on security or performance

Quiz 5.

1. One of the BadStore pages has a hidden form field that establishes a new user's privilege level. What is the name of this field?

ans: role

2. How many items for purchase are in BadStore's database? Use SQL injection on the quick search form field to find out.

ans: \*\*\*16 \*\*\*

3. Which of the following operations are suppliers permitted to do? Use SQL injection to bypass authentication, or find a way to create an account as a supplier.

**View existing price list**

Cancel contract

**Upload price list**

Submit monthly bill payment

Download an activity report

ans: 'OR 1=1 OR'

4. Log in as joe@supplier.com --- this is possible in a variety of ways, including SQL injection. Then look at his previous orders and answer the question: What credit card number did he use to make a purchase of $46.95? Multiple answers are possible, but we will accept all of them.

ans: 5500000000000004

4. Get administrator privileges and then use the admin action to look at the user database. There are two users whose emails have the form XXX@whole.biz; what is the XXX portion of either of the two users? For example, if one of the users is jackie@whole.biz, the right answer is jackie. (The answer is case-sensitive.)

ans: fred

5. BadStore uses cookies to implement a session key, once you've authenticated, and for tracking the contents of the cart, once you've added something to it. You can figure out the cookies in use by BadStore in various ways. One way is to do an XSS attack on the guest book. Get the guest book to run the code <script>alert(document.cookie)</script> and it will tell you the current cookies. (Be sure you have popups enabled on your browser or this won't work.) Alternatively, you can examine the cookies directly using Firefox developer tools. Recall that cookies are pairs key=value. What is the key of the session cookie?

ans: SSOid=YWRtaW46NWViZTIyOTRlY2QwZTBmMDhlYWI3NjkwZDJhNmVlNjk6TWFzdGVyIFN5c3RlbSBBZG1p%0AbmlzdHJhdG9yOkE%3D%0A; CartID=1416121184%3A2%3A4010.5%3A1000%3A1004

**SSOid**

6. What is the key of the cookie used for the cart?

ans: CartID

7. BadStore's session cookie format is poorly designed because it is uses a predictable structure. In particular, it is an encoded string (with a URL-encoded newline at the end) of the form XXX:YYY:ZZZ:U. What are the XXX, YYY, and ZZZ portions of this string?

ans: e-mail address

MD5 hash of password.

Full name

Role.

8. BadStore's cart cookie is also an encoded string with a predictable structure XXX:YYY:... etc., and it probably contains information it shouldn't. Which field of the decoded string could an attacker change to give himself a discount on an item's price?

ans: 3

Quiz 6.

1. What is one difference between an HTTP GET and an HTTP POST request?

Only GET requests use the REFERER header

**Only POST requests may include parameter data in the request body**

Only GET requests are subject to the same-origin policy

Only POST requests can encode parameters in the URL

2. Which of the following is true about static and dynamic web content?

Static pages may include PHP programs, which execute at the browser

**The server often produces dynamic content based on the contents of the database**

Static content may be re-generated with each request

Javascript programs embedded in HTML pages are run server-side to produce dynamic content

3. SQL injection exploits a bug in what interaction of a web application?

Client to server

Network to server

Server to client

**Server to database**

4. SQL injection often allows an attacker to do which of the following?

Overrun a buffer to smash the stack

All of the above

Cause memory to be used after it's freed

**Access information he shouldn't**

5. If you had to summarize the key (most specific) programming failure with SQL injection, it would be:

**Confusing data with code**

Bypassing authentication

Trusting without verifying

Circumventing the same origin policy

6. What is escaping an example of?

Blacklisting

**Sanitization**

Checking

Whitelisting

7. Suppose a web application implements authentication by constructing an SQL query from HTML from data using PHP's prepared statements. What would happen if an attacker entered FRANK' OR 1=1; -- in the web form's user field?

The text will modify the structure of the SQL query and possibly bypass authentication

The text will be confused as the password and authentication will probably fail

The text will corrupt the query structure and the database will view it as a syntax error

**The application will try to authenticate a user whose name is FRANK' OR 1=1; --**

8. Why is it undesirable to implement session identifiers using (only) hidden form fields?

Such fields cannot include timeout information

Such fields cannot contain binary data

These fields are easily modified by the user

**The session ID is forgotten when the browser window is closed**

9. Suppose a browser submits a GET request to URL http://www.mybank.com/accountinfo on 20 February 2015. Which of the following cookies, if already stored at the browser, would be sent with the request?

lang=us-english; expires=Sat, 1-Aug-2015; path=/accountinfo/; domain=.fidelity.com

editon=us; expires=Thu, 19-Feb-2015; path=/accountinfo/prefs; domain=.mybank.com

edition=us; expires=Wed, 18-Feb-2015; path=/; domain=.mybank.com

**sessid=ABCDEFG; expires=Sat, 21-Feb-2015; path=/; domain=.mybank.com**

10. Which of the following are ways that session cookies could be stolen or forged?

Stealing it from the password database

**Predicting the cookie's structure and reconstructing it**

**Reading a cookie from an unencrypted web request**

11. Which of the following are ways to reduce the impact of a stolen cookies?

Prevent cookies from entering the DNS cache

Giving each cookie a timeout

**Changing a user's cookie from session to session**

12. How can the REFERER field be used to defend against CSRF attacks?

**It can be used to ensure that sensitive requests are (only) initiated by interaction with a site's own pages**

It ensures that requests only come from authenticated users

It can't be used reliably because it only works for dynamic content

It can be used to check that a Javascript program is from the proper origin

13. <script></script>tags in HTML pages most often identify programs written in what language?

PHP

C

Java

**Javascript**

14. The browser implements security for Javascript programs for what reason?

**Such programs may access browser-controlled resources, which include potentially sensitive data in HTML documents and cookies**

It doesn't -- these programs are only used to render dynamic content but are otherwise not security-relevant

Such programs could deny service by running forever

It doesn't -- Javascript programs run at the server so the browser can ignore them

15. XSS subverts what policy?

Whitelisting

**Same Origin**

Availability

Secure defaults

16. What is the difference between stored (or persistent) XSS and reflected XSS?

Stored XSS works by injecting code in a site's served content, while reflected XSS injects code in a URL

**Stored XSS works on database queries while reflected XSS works on cookies, which are received from and reflected back to the server**

Stored XSS embeds Javascript in an a URL, while reflected XSS embeds it in a mirrored site

Stored XSS is amenable to blacklisting but reflected XSS is not.

Quiz 7.

1. Why is waiting to think about security until after the software is built a bad idea?

**All of the above**

Fixing problems once the software is built is more difficult and more expensive

You might miss important security requirements that necessitate a re-design

You might make critical mistakes in the software's design

2. What is an abuse case?

An official report made by MITRE Corp that describes a discovered software vulnerability and possible abuse of it

**A scenario that illustrates a potential failure in security under relevant circumstances**

An example of a heated disagreement between the security team and the development team

A scenario that illustrates a system's functional requirements

3. Which of the following is a reason to make an explicit threat model when designing a system?

So that you avoid an incoherent defense

So you can defend against the most likely/costly/important attacks

So you can explicitly list and challenge assumptions that underlie your design

**All of the above**

4. Suppose you design software for a bank and the bank's customers may remotely log into its site using commodity PCs. These PCs might have malware on them, which could log keystrokes or read files stored on the machine. Which threat model (using terms defined in the lectures) makes the most sense for you to consider, when designing the bank's site?

Malicious user

**Co-located user**

Network user

Snooping user

5. What is a good defense against powers that are particular to a snooping user?

**Using encryption**

Using a firewall

Using passwords to authenticate users

Using a type-safe language

6. A denial of service attack violates what security policy/goal?

Integrity

**Availability**

Authorization

Authentication

7. When talking about computer security, what do we mean by the term, principal?

**An actor, or role, that is the subject of a security policy**

A rule of thumb for secure coding

A method for delegation

A foundational observation

8. Passwords, biometrics, and user-owned SMS-receiving mobile phones are useful for what security mechanism?

Small trusted computing base (TCB)

Audit

Authorization

**Authentication**

9. We identified several categories of secure design principles, with respect to how they deal with attacks. Running each browser tab in a separate OS process (as done by the Chrome browser) is an example of which category?

Prevention (of an attack)

**Mitigation (of the damage from an attack)**

Recovery (from a successful attack)

None of the above

10. Suppose you are implementing a graphical user interface for interacting with an implementation of the RSA cryptosystem, and you want to give users a way to generate new keys. Which of the following designs most takes security into account?

**Allow the user to use a slider to choose the number of bits, setting slider initially to point at 2048 bits. As the user moves the slider to larger or smaller values, visualize the difference in relative protective power, e.g., using a meter.**

Use a text box to ask the user to fill in how many bits they want their key to be

Don't ask the user about key size at all -- always use 256 bits

Ask the user, but set the default response to be 2048 bits, which is chosen based on the assumption of a strong adversary

11. Suppose you are implementing an extensible data management system. You want to accommodate plug-ins that can implement storage rules and query processing functionality for different data formats (e.g., relational data, object data, XML data, etc.). Which of the following designs most takes security into account?

The plug-ins and the main data management software are linked into the operating system kernel as a special kind of device driver, to give them direct access to stable storage and the network stack, while the OS can enforce their security

The plug-ins are linked directly in the address space of the data management software, ensuring high performance

**The plug-ins are implemented as separate OS processes; these processes communicate to/from the main process to handle queries/updates for the data formats they support**

The plug-ins are implemented as separate OS processes but which share memory with the main process (and may access its memory as well), for better efficiency. Queries/updates occur via inter-process communication.

12. Promoting privacy is a goal that follows from which category of secure design principle?

**It is an example of trusting with reluctance because promoting privacy means sharing private information with as few software components as possible, meaning that fewer need to be trusted to protect the information**

It is an example of defense in depth because privacy is a deep topic that is often debated.

It is an example of monitoring and recovery because failure to promote privacy could be discovered by monitoring

It is an example of favoring simplicity because privacy is quite simply the right thing to do

13. Encrypting a password database is an example of what category of design principle?

**It is an example of defense in depth**

It is an example of favoring simplicity

It is an example of monitoring and recovery

14. Which of the following vulnerabilities can VSFTPD's secure string library help protect against?

Privilege escalation

**Buffer overflow**

**Integer overflow**

15. VSFTPD forks a new process to handle each client connection. It could have, instead, spawned a thread within the main process to handle each connection, as is done in many servers. How would this alternative design compare to the original?

**It would be less secure because a compromise by a malicious client in one thread could (more easily) access data used by another client's thread, since they share the same address space**

It would be equally secure and would perform better because threads are cheaper to manage than processes

It would be more secure because threads are not subject to denial of service attacks but processes are

It would be more secure because we could apply the SecComp system call to these threads, but could not do so for processes

16. FTP servers can be asked to list a directory of files. VSFTPD could do this by calling the system's ls (or dir) command, displaying the result to a client. But VSFTPD does not do this, and implements directory listings using the relevant system calls directly. Why might you argue that VSFTPD's design makes sense from a security perspective?

**ls does more than is needed, and thus unnecessarily expands the TCB**

Calling ls involves forking a new process, which is less secure than running within the same process

Calling ls doesn't give us any way to employ fail-safe defaults

Using ls provides less control over the output, which leaves users open to XSS-style attacks

Quiz 8.

1. How many iterations does it take the fuzzer to find the bug (i.e., record a crash)? What is the string that it discovers crashes the program?

ans: 0

2. how many iterations?

ans: 1000

3. Name one symbolic variable that was set in the path condition identified by KLEE that crashes wisdom-alt2

ans: buf

4. Name another symbolic variable set in the path condition identified by KLEE that crashes wisdom-alt2.

ans: r

5. Which symbolic variables were involved (AAAAAA and BBBBBB in the above)?

ans: buf, \x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00

6. What was their contents (XXXXXXXX in the above)?

ans: \x00\x00\x00\x00

7. What was the data (the XXXXetc. part, not including any \x00\x00 parts, if any) for the program object?

ans: sddwddddssssddwwww

8. If you run the symbolic maze program so that it finds all solutions, not just one, how many are there?

ans: 4

9. There was a bug in the maze program that allows the player to walk through walls. What line in maze-sym.c is the bug on? (If there are multiple lines, pick one of them.)

ans: 113

Quiz 9.

Project 3 quiz

1. Does fuzz.py identify a crash in wisdom-alt? In how many iterations?

Identifies a crash, 44 iterations

Does not identify a crash

Identifies a crash, 103 iterations

**Identifies a crash, one iteration**

2. Does fuzz.py identify a crash in wisdom-alt2? In how many iterations?

**Does not identify a crash**

Identifies a crash, 133 iterations

Identifies a crash, 800 iterations

Identifies a crash, 1 iteration

3. Name one symbolic variable that was set in the path condition identified by KLEE that crashes wisdom-alt2.

Enter answer here

**buf**

4. Name another symbolic variable set in the path condition identified by KLEE that crashes wisdom-alt2.

Enter answer here

**r**

5. What was the data content of the buf object?

'\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\xFF\x00\x00\x00\x00\x00\x00\x00\x00\xAA'

**'\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00'**

'\xFF\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00'

'\x00\x00\x00\xFF\x00\x00\x00\x00\x00\x00\xBB\x00\x00\x00\x00\x00\x00\x00\x00\xEE'

6. After executing the symbolic maze, what was the data value of the 'program' object? (Hint: it will be a string of the lowercase letters s, d, w, and a.)

Enter answer here

**sddwddddsddw**

7. If you run the symbolic maze program so that it finds all solutions, not just one, how many are there?

Enter answer here

**309**

8. There was a bug in the maze program that allows the player to walk through walls. What line in maze-sym.c is the bug on? (If there are multiple lines, pick one of them.)

Enter answer here

**113**

Quiz 10.

1. A static analysis

is a kind of real analysis for solving numeric equations

analyzes the fixed, or static portions of a program

is always better than testing

**analyzes a program's code without running it**

2. Which of the following are advantages of static analysis over testing?

A static analysis runs faster than testing

A static analysis is more precise than testing

**A static analysis can analyze programs that are not necessarily executable on their own, e.g., libraries**

3. The halting problem is the problem of determining, for an arbitrary program and input, whether the program will finish running or continue to run forever. Which of the following statements about the halting problem are true?

You cannot build an automated analysis that proves that a particular program P terminates.

**Many other program analysis problems can be converted to the halting problem.**

You cannot solve the halting problem with static analysis, but you can with symbolic execution.

4. Suppose we have a static analysis that aims to find buffer overflows in C programs. If the analysis is sound, then which of the following is true about it?

**It may have false alarms, but will not fail to report actual bugs**

It will not have any false alarms, but may fail to report actual bugs

It will report all actual bugs, and have no false alarms

It may miss bugs, and have false alarms

5. A tainted flow is

**A flow from an untrusted source to both trusted and untrusted sinks**

A flow from an untrusted source to a trusted sink

A flow from a trusted source to an untrusted sink

A flow from a trusted source to both trusted and untrusted sinks

6. (4 points) Consider the program below, using the qualified types annotations for tainted flows given in the lecture (shown in comments). In particular, notice that the variable fmt and the argument to printf are untainted, while the result of fgets is tainted. Suppose we analyze this with a tainted flow analysis. This program has no bugs, but which kinds of analysis report a false alarm?

/\* int printf(untainted char \*fstr, ...); \*/

/\* tainted char \*fgets(...); \*/

char \*chomp(char \*s) {

int i, len = strlen(s);

for (i = 0; i<len; i++)

if (s[i] == '\n') {

s[i] = '\0';

break;

}

return s;

}

void foo(FILE \*networkFP, untainted char \*fmt) {

char buf[100];

char \*str = fgets(buf, sizeof(buf), networkFP);

char \*str1 = chomp(str);

char \*fmt1 = chomp(fmt);

printf(fmt1,str1);

}

**flow-sensitive, context-sensitive**

path-sensitive, context-sensitive

flow-sensitive, context-INsensitive

**flow-INsensitive, context-INsensitive**

7. (4 points) Consider the following code, where the referenced chomp function is the same as in the previous question. Suppose we analyze this with a tainted flow analysis. Once again, this program has no bugs, but which kinds of analysis report a false alarm?

void bar(FILE \*networkFP, char \*fmt, int testing) {

char buf[100];

char \*str = fgets(buf, sizeof(buf), networkFP);

char \*str1 = chomp(str);

if (testing)

str1 = "test format";

printf(fmt,str1);

if (testing)

printf(str1);

}

**flow-sensitive, context-sensitive**

path-sensitive, context-INsensitive

**flow-sensitive, context-INsensitive**

flow-INsensitive, context-INsensitive

8. Which of the following are true of implicit flows?

**One can occur when assigning an untainted value to an untainted variable, but conditioned on a tainted value**

**Implicit flows are rarely detected by tainted flow analyses, because detecting them can increase false alarms**

They only arise in object-oriented languages with dynamic dispatch, since the choice of method to call is implicit

9. What is a key advantage of symbolic execution over static analysis?

Symbolic executors consider all possible program runs, while static analyses don't

**As a generalized form of testing, when a symbolic executor finds a bug, we are sure it is not a false alarm**

Symbolic executors can consider partial programs (e.g., libraries) while static analyzers cannot

Symbolic executors are both sound and complete, while static analyzers can only be one or the other

10. Symbolic execution, viewed as a kind of static analysis, has which of the following "sensitivities?"

Flow-sensitivity

Context-sensitivity

Path-sensitivity

**All of the above**

11. Why is concolic execution problematic for non-terminating programs?

**Its search strategy is to choose new test cases based on constraints generated by terminating runs**

Concolic execution takes a breadth-first approach, but non-terminating programs are better suited to a depth-first approach

Non-terminating programs will consume too many resources

Non-terminating programs require user interaction, which concolic execution does not handle

12. Suppose that x and y in the following program are symbolic. When the symbolic executor reaches the line that prints "everywhere" what will the path condition be?

/\* assume x and y are both symbolic \*/

void foo(int x, int y) {

if (x > 5) {

if (y > 7) {

printf("here\n");

} else {

if (x < 20)

printf("everywhere\n");

else

printf("nowhere\n");

}

}

}

¬(y > 7) ∧ x < 20

x > 5 ∧ ¬(y > 7) ∧ ¬(x < 20)

**x > 5 ∧ ¬(y > 7) ∧ x < 20**

x > 5 ∧ y > 7 ∧ x < 20

13. Suppose that x in the following program is symbolic. When the symbolic executor reaches the line that prints "here" what will the path condition be?

void bar(int x) {

int z;

if (x > 5)

z = 5;

else

z = 1;

if (z > 3)

printf("here\n");

}

x > 5 ∧ z > 3

**x > 5**

¬(x > 5) ∧ z > 3

z > 3

14. Which of the following are heuristics that symbolic executors use to cover more of the search space?

Switch between concolic and non-concolic execution

**Choose between two paths based on a notion of priority**

**Choose between two paths based on whether one reaches program statements not previously executed**

Quiz 11.

1. What is penetration testing?

A procedure for testing libraries or other program components for vulnerabilities

All of the above

**Whole-system testing for security flaws and bugs**

A security-minded form of unit testing that applies early in the development process

2. Which of the following are benefits of penetration testing?

You can prove a positive: Penetration testing will establish your system is secure

Compositionality of security properties means tested components are secure even if others change

**They specifically consider adversarial thinking, which is not usually necessary for normal tests**

Results are often reproducible

3. What does it mean to "be stealthy" during a penetration test?

Performing the tests from an undisclosed location

**Taking care to avoid activities during a penetration test that might attract attention, e.g., by operators or IDS services**

Using encryption during tests to make the source of attacks impossible to determine

Performing penetration testing without the target organization knowing

4. What is a web proxy?

**A piece of software that intercepts and possibly modifies requests (and responses) between a web browser and web server**

An agent that makes decisions on the client's behalf when interacting with web applications

A piece of software that makes a web application look like a standalone application, making it easier to test

A simulator for the web, for use when off-line

5. What is Nmap?

**It is a scanner which works by injecting packets to a range of addresses, and inferring what hosts and services might be at those addresses, based on the responses**

It is a map of the Internet

It is a network fuzz testing tool

It is a suite of tools for scripting attacks: probe, construct, encode, inject, wait for response

6. What is ethical hacking?

Hacking into systems run by those whose ethics you disagree with

"Hacking" ethics so they justify unintended selfish behavior

**Hacking systems (e.g., during penetration testing) to expose vulnerabilities so they can be fixed, rather than exploited**

A slang term for rapid software development, e.g., as part of hackathons

7. Which of the following statements describe fuzz testing (aka fuzzing)?

**It is concerned with finding known-bad behaviors, like crashes and hangs**

It focuses on simple testing patterns and does not employ sophisticated analysis techniques

It is always black-box, in being indifferent to the software's functionality

**It has been used to find security vulnerabilities in many commodity programs**

8. Which of the following are true of whitebox fuzzing?

**It takes into account the program's internals in some manner when deciding which inputs to choose**

Radamsa is (at least in part) a whitebox fuzzer

**SAGE is (at least in part) a whitebox fuzzer**

It makes no sense to combine it with grammar-based fuzzing since the latter is just another way to consider the program's semantics

9. Which of the following is true of mutation-based fuzzing?

It only makes sense for file-based fuzzing, not network-based fuzzing

Each input is mutation that follows a given grammar

It works by making small mutations to the target program to induce faults

**It generates each different input by modifying a prior input**

10. Which of the following styles of fuzzer is more likely to explore paths covering every line of code in the following program?

Blackbox

**Whitebox**

Mutation-based

Generational

11. Which of the following are functions of a network-based fuzzer?

Scanning a network address range

**Acting as a "man in the middle"**

**Acting as a server**

12. Suppose you want to use fuzzing on a program to try to find memory errors; which of the following statements is true?

Fuzzing doesn't find memory errors, it finds crashes and hangs

You should not use a grammar-based fuzzer, because its adherence to the grammar means it will not find memory errors

Compiling the program with address sanitizer (ASAN) will make errors harder to reproduce

**Compiling the program with address sanitizer (ASAN) will make the source of a memory error easier to find**

Consider the Vigenere cipher over the lowercase English alphabet, where the key length can be anything from 8 to 12 characters. What is the size of the key space for this scheme?

**- 26^8 + 26^9 + 26^10 + 26^11 + 26^12**

Consider the Vigenere cipher over the lowercase English alphabet, where the key has length 8. For which of the following message spaces will this scheme be perfectly secret? (Check all that apply.)

**- - The set of all 8-character strings of lowercase English letters.**

**- The set of all 7-character strings of lowercase English letters**.

What is the result of encrypting the ASCII plaintext "cool!" using the variant Vigenere cipher (where encryption is done using byte-wise XOR) and key 0x01 3F?

**- 0x62 50 6E 53 20**

Say we have a scheme with a claimed proof of security with respect to some definition, based on some assumption. The scheme was successfully attacked when used in the real world. What are possible reasons for this? (Check all that apply.)

**- - The assumption may be false.**

**- The proof might be incorrect.**

**- The definition of security may not correctly capture the real-world threat model.**

In the definition of perfect secrecy, what threat model is assumed?

**- The attacker can eavesdrop on a single ciphertext.**

Consider the Vigenere cipher over the lowercase English alphabet, where the key can have length 1 or length 2, each with 50% probability. Say the distribution over plaintexts is Pr[M='aa'] = 0.4 and Pr[M='ab'] = 0.6. What is Pr[C='bb']? Express your answer to 4 decimal places with a leading 0, i.e., if your answer was 1/2 then you would enter 0.5000 (without a trailing period).

**- 0.0084**

Consider the Vigenere cipher over the lowercase English alphabet, where the key can have length 1 or length 2, each with 50% probability. Say the distribution over plaintexts is Pr[M='aa'] = 0.4 and Pr[M='ab'] = 0.6. What is Pr[M='aa' | C='bb']? Express your answer to 4 decimal places with a leading 0, i.e., if your answer was 1/2 then you would enter 0.5000 (without a trailing period). Note: carry out the calculation exactly (i.e., do not use the truncated result that you entered as your answer in the previous question) before truncating your answer to 4 decimal places.

**- 0.9473**

Which of the following are true for obtaining perfect secrecy using the one-time pad, assuming the message space contains messages all of some fixed length? (Check all that apply.)

**- - The key must be as least as long as the messages in the message space.**

**- The key should be chosen uniformly.**

**- The key should be shared between the two communicating parties, and kept secret from any potential attacker.**

Consider the one-time pad over the message space of 5-bit strings, where Pr[M=00100] = 0.1 and Pr[M=11011] = 0.9. What is Pr[C=00000]? Express your answer to 5 decimal places with a leading 0. I.e., if your answer was 1/2, then you would enter 0.50000 (without a trailing period).

**- 0.03125**

Which of the following are true about the Vigenere cipher? (Check all that apply.)

**- The Vigenere cipher is perfectly secret if the length of the key is equal to the length of the messages in the message space.**

Two ASCII messages containing English letters and spaces only are encrypted using the one-time pad and the same key. The 10th byte of the first ciphertext is observed to be 0xB7 and the 10th byte of the second ciphertext is observed to be 0xE7. Let m1 (resp., m2) denote the 10th ASCII character in the first (resp., second) message. What is the most you can conclude about m1 and m2?

**- One of m1 or m2 is the space character, and the other is the character 'p'.**

Three ASCII messages containing English letters and spaces only are encrypted using the one-time pad and the same key. The 10th byte of the first ciphertext is observed to be 0x66, the 10th byte of the second ciphertext is observed to be 0x32, and the 10th byte of the third ciphertext is observed to be 0x23. Let m1 (resp., m2, m3) denote the 10th ASCII character in the first (resp., second, third) message. What is the most you can conclude about m1, m2, and m3?

**- m1 is the space character, m2 is the character 't', and m3 is the character 'e'**.

Which of the following is true about computational secrecy? (Select all that apply.)

**- - Computational secrecy allows an attacker to learn information about the message with small probability.**

**- Computational secrecy currently relies on unproven assumptions.**

**- Computational secrecy only ensures secrecy against attackers running in some bounded amount of time.**

Let G be a function mapping n-bit inputs to 2n-bit outputs. Which of the following is true of the pseudo one-time pad encryption scheme based on G? (Check all that apply.)

**- The scheme is computationally secret if G is a pseudorandom generator.**

Which of the following attackers can be used to demonstrate that the shift cipher for 3-character messages does not satisfy perfect indistinguishability?

**- Output m0 = 'aaa' and m1 = 'abc'. Given challenge ciphertext C, output 1 if the three characters of C are all different.**

Which of the following is a negligible function? (Check all that apply.)

**- - f(n) = 1/2^n**

**- f(n) = n/2^n**

Define the following function G taking n-bit inputs and producing (n+1)-bit outputs: G(x)=x∥0, where ∥ denotes concatenation. Which of the following attackers shows that this G is not a pseudorandom function?

**- On input an (n+1)-bit string y, output 0 if the last bit of y is 0.**

Say G is a pseudorandom generator taking n-bit inputs and producing 2n-bit outputs. Which of the following are necessarily true? (Check all that apply. The symbol '|' is used here for string concatenation.)

**- G(r) is computationally indistinguishable from a uniform, 2n-bit string if r is a uniform n-bit string.**

Which of the following is a setting in which a pseudorandom generator could be applied?

**- You have a way to generate random bits at the rate of 100 bits/second, but you need 1,000,000 random bits to run a statistical simulation.**

Consider a pseudo one-time pad encryption scheme Π constructed using some function G. Which of the following did our proof of security for the pseudo one-time pad show?

**- If G is a pseudorandom generator, then Π is computationally secret.**

True or false: any private-key encryption scheme that is CPA-secure must also be computationally indistinguishable.

**- True**

True or false: any private-key encryption scheme that is CCA-secure must also be perfectly secret.

**- False**

True or false: any private-key encryption scheme that is CCA-secure must also be CPA-secure.

**- True**

Let F be a block cipher with 128-bit block length. Consider the following encryption scheme for 256-bit messages: to encrypt message M=m1∥m2 using key k (where |m1|=|m2|=128), choose random 128-bit r and compute the ciphertext r∥Fk(r)⊕m1∥Fk(m1)⊕m2. Which strategy would lead to a valid chosen-plaintext attack?

**- Let m1 and m2 be arbitrary but distinct. Using the encryption oracle, obtain an encryption r∥c1∥c2 of m1∥m2. Output messages M0=m1∥m2 and M1=m2∥m1. Output 0 if the third block of the challenge ciphertext is c2**

Let F be a pseudorandom function with 128-bit key and 256-bit block length. Which of the following functions G are necessarily pseudorandom generators? (Select all that apply.)

**- - G(x)=Fx(0...0)∥Fx(1...1), where x is a 128-bit input.**

**- G(x)=Fx(0...0), where x is a 128-bit input.**

Define the keyed function F as follows: Fk(x)=k⊕x. Which of the following distinguishers demonstrates that F is not a pseudorandom function?

**- Given access to an oracle g, query y0=g(0...0) and y1=g(1...1). Then output 1 if and only if y0⊕y1=1...1.**

Let F be a block cipher with n-bit block length. Consider the following encryption scheme: to encrypt a message viewed as a sequence of n-bit blocks m1,m2,...,mt using a key k, choose a random n-bit value r and then output the ciphertext r,Fk(r+1+m1),Fk(r+2+m2),...,Fk(r+t+mt), where addition is done modulo 2n. Which of the following attackers demonstrates that this scheme is not computationally indistinguishable:

**- Let m be an arbitrary n-bit block, and output M0=m,m and M1=m,m−1. Given challenge ciphertext r,c1,c2, output 1 if and only if c1=c2.**

Say we use CBC-mode encryption based on a block cipher with 256-bit key length and 128-bit block length to encrypt a 512-bit message. How long is the resulting ciphertext?

**- 640 bits**

Assume an honest user wants to send an 8-bit integer to their bank indicating how much money should be transferred to the bank account of an attacker. The user uses CTR-mode encryption based on a block cipher F with 8-bit block length. (Yes, this is a made-up example.) The attacker knows that the amount of money the user wants to transfer is exactly $16, and has compromised a router between the user and the back. The attacker receives the ciphertext 10111100 01100001 (in binary) from the user. What ciphertext should the attacker forward to the bank to initiate a transfer of exactly $32? (Recall that CTR-mode decryption of a ciphertext c0,c1 using key k is done by outputting c1⊕Fk(c0+1).)

**- 01100001 10111100**

Assume CTR-mode encryption with PKCS #5 padding and a block cipher with 8-byte block length. Say a 4-byte message is encrypted, resulting in ciphertext 0x00 01 02 03 04 05 06 07 00 01 02 03 04 05 06 07. Which of the following ciphertexts will NOT yield an error upon decryption?

**- 0x00 01 02 03 04 05 06 07 00 01 02 04 04 05 06 07**

True or false: CBC-mode encryption with PKCS #5 padding provides message integrity, as long as the receiver makes sure to verify the padding upon decryption.

**- False**

Consider the message authentication code for 2n-bit messages definedby Mack(m1,m2)=Fk(m1)⊕Fk(m2). Which of the following gives a valid attack on this scheme?

**- Obtain tag t on message 1,2m1​,m2​ (with 1≠2m1​​=m2​), and then output the tag t on the message 2,1m2​,m1​.**

Consider the message authentication code for 2n-bit messages definedby Mack(m1,m2)=Fk(m1)⊕Fk(m2). Which of the following gives a valid attack on this scheme?

- **Output the tag 0...0= on the message 0...0, 0...0**

Assume a sender and receiver use basic CBC-MAC but authenticate/accept messages of different lengths. Which of the following is a valid attack?

**- Obtain tag t1​ on message m1​, and tag t2​ on message m1​,m2​. Then output the tag t2​ on the message t1​⊕m2​.**

Assume we want to use a hash function with output length as small as possible, subject to being collision resistant against a birthday attack running in time 2^192. Which hash function would be the best choice?

**- SHA-3 with 384-bit output.**

Let H,H′ be collision-resistant hash functions. Which of the following functions H′′ is NOT necessarily collision-resistant?

**- H′′(x)=H(x)⊕H′(x).**

Assume a sender and receiver use the encrypt-and-authenticate approach for variable-length messages, using CTR-mode encryption and a variant of CBC-MAC secure for authenticating variable-length data (and independent keys for each). Which of the following statements is true?

**- The combination is not CPA-secure, but it does provide integrity.**

Let F be a block cipher with block length n. Consider the following encryption scheme for n-bit messages: to encrypt message m using key k, choose a random c0​∈{0,1}^n and output the ciphertext c0​,c1​,Fk​(Fk​(c0​)⊕c1​), where c1​=Fk​(c0​)⊕m. Which of the following statements is true?

**- This looks like the encrypt-then-authenticate approach using CTR-mode and CBC-MAC, except that here the same key is being used for both -- Prof. Katz warned us about that; this looks insecure!**

Which of the following is the most appropriate primitive for achieving message integrity between two users sharing a key?

**- Message authentication code (MAC)**

Which of the following is an example of a message authentication code used widely in practice?

**- HMAC**

Consider the following algorithm for factoring an integer N provided as input (in binary): Fori=2to⌈N−−√⌉, ifidividesN, then output(i,N/i). Which of the following statements is true?

**- This algorithm is correct, but it runs in exponential time.**

Which of the following is NOT a group?

**- The integers under multiplication.**

Which of the following is the multiplicative inverse of 10 modulo 15?

**- There is none, since gcd⁡(10,15)≠1**

What is [5^80 mod79]? (Note that 79 is prime. Don't use a calculator/computer!)

**- 25**

How many elements are in the group Z\*403​? (Note that 403=13⋅31.)

**- 360**

Which of the following gives the 3rd root of 92 modulo 187? (Note that 187=11⋅17.)

**- [92^107 mod 187]**

Which of the following problems is hard if the RSA assumption holds? In all the below, N is a product of distinct, large primes p and q, and e is relatively prime to ϕ(N).

**- Given N, e, and a uniform value y∈ZN∗​, find x such that x^e=y mod N.**

Which of the following is a generator of Z13∗​?

**- 2**

Z23∗​ is a cyclic group with generator 5. In this group, what is DH5​(2,20)?

**- 9**

Let G be a cyclic group of order q and with generator g. Based only on the assumption that the discrete-logarithm problem is hard for this group, which of the following problems is hard?

**- Given a uniform y∈G, find x such that gx=y.**

Which of the following is a drawback of the private-key setting that is NOT addressed by the public-key setting?

**- The communicating parties need the ability to generate random bits.**

Which of the following BEST describes the security offered by the Diffie-Hellman key-exchange protocol (assuming the DDH problem is hard)?

**- An attacker eavesdropping on an execution of the protocol cannot distinguish the key shared by the parties from a uniform key.**

Assume the Diffie-Hellman protocol is run by two parties in the subgroup of Z23∗​ generated by 2. (This subgroup has order 11.) If the first party chooses private exponent 3 and the second chooses private exponent 10, which of the following characterizes the execution of the protocol in this case?

**- The first party sends 8, the second party sends 12, and they share the key 3.**

In which of the following scenarios is public-key encryption a better choice than private-key encryption?

**- A user wants to send his credit-card number to a merchant on the web.**

Which of the following would NOT be a secure way for a receiver to distribute her key for a public-key encryption scheme? (Assume a passive, eavesdropping attacker here.)

**- Post the private key on one's webpage.**

Which of the following is true in the public-key setting, but NOT true in the private-key setting?

**- Allowing the attacker to have access to an encryption oracle makes no difference when defining security.**

Assume for the purposes of this question a public-key encryption scheme for which the time to encrypt a 128-bit message is 100 times slower than the time to compute one AES evaluation. Which of the following is true if we want to encrypt a 100MB message M?

**- If hybrid encryption is used, then public-key encryption of M will take roughly the same time as private-key encryption of M.**

Assume El Gamal encryption, where the group being used is Z47∗​ with generator 5. (This group has order 46, which is not prime. But El Gamal encryption can be defined in any cyclic group.) Assume the public key contains h=10. Say an attacker sees a ciphertext (41, 18) that is the encryption of some unknown message m. Which of the following is an encryption of [5m mod47]?

**- (41, 43)**

Assume "plain RSA" encryption is used with public key (N=33,e=3). What is the encryption of the message m=2?

**- 8**

Which of the following is true about "plain RSA" encryption (assuming the RSA problem is hard)?

**- If the message m is uniform in ZN∗​, then m cannot be recovered in its entirety from the ciphertext in polynomial time.**

The Federal Government wants to be able to issue advisories to the general public while ensuring that no one will be able to tamper with their messages or spoof a fake advisory. Which of the following is the best cryptographic approach to address this problem?

**- Use a digital signature scheme, with the public key known to everyone, to sign each advisory when it is released**.

The president and vice president of a company want to communicate while ensuring integrity of their communication. Which of the following is the best cryptographic approach to address this problem?

**- Use a message authentication code, with the key shared between them, and generate a tag for each message they send.**

Assume for the purposes of this question a digital signature scheme for which the time to sign a 256-bit message is 100 times slower than the time to evaluate SHA-256 on a 512-bit input. Which of the following is true if we want to sign a 500MB message M?

**- If the hash-and-sign approach is used, then signing M will take roughly the same time as hashing M.**

Assume the "plain" RSA signature scheme, with public key (N=55,e=3). Which of the following verifies correctly as the signature on the message m=17?

**- 8**

Assume the "plain" RSA signature scheme with public key (N,e=3). For which of the following messages is it always possible to forge a signature without seeing any prior signatures or factoring N? (Assume N>1000, and N relatively prime to each of the messages that follow.)

**- 27**

Assume the "plain" RSA signature scheme with public key (N,e). Say we want to forge a signature on m=289 but can only obtain a signature on one other message. Which of the following strategies will work? (Assume N>1000.)

**- Obtain signature σ on m′=17. Output [σ2modN] as the signature on m.**

In this and the next question, assume the Schnorr identification protocol is run in the subgroup of Z23∗​ generated by 2. (This subgroup has order 11.) Say the prover's private key is x=7. What is the prover's public key?

**- 13**

(This is a continuation of the previous question.) Say the prover runs an execution of the Schnorr identification protocol with a verifier. The prover chooses r=4 and sends A=16. The verifier sends challenge 33. What response does the prover send?

**- 3**

As in the lectures, let certA→B​ denote a certificate issued by A for B, i.e., certA→B​=SignskA​​(B,pkB​). Assuming D knows pkC​ and trusts C, which of the following provides evidence to D that A's public key is pkA​?

**- certC→B​, pkB​, certB→A​, and pkA​.**

Consider the SSL/TLS handshake protocol as described on slide 5 of the SSL/TLS lecture. Say the encryption of pmk were changed from using a CCA-secure public-key encryption scheme to using a CPA-secure public-key encryption scheme. Which of the following attacks would this change potentially enable?

**- An attacker can eavesdrop on an execution of the protocol to learn the ciphertext c. Then, it can impersonate the client, send modified versions of c to the server, and learn pmk by using information about whether the server returns an error or not in response to these ciphertexts.**

What was your favorite part of this class?

**- Encryption**

What is the most appropriate cryptographic primitive to use if a company wants to distribute authenticated software updates to its customers?

**- Digital signature scheme.**

What is the most appropriate cryptographic primitive to use if an individual wants to ensure confidentiality of the files stored on her hard drive?

**- Private-key encryption.**

A user wants to design a CPA-secure public-key encryption scheme to be used for emailing large files. Of the following, which would be the best approach?

**- To encrypt a file, use El Gamal encryption to encrypt a random AES key; then use AES (with that key) in CBC mode to encrypt the file.**

Consider the following "hybrid" signature scheme, which will give better efficiency when signing long messages. To sign message M using private key sk, choose a uniform key k for a message authentication code and then send k,Signsk​(k),Mack​(M). Verification is done in the natural way. Which of the following is true regarding this scheme?

**- This is not secure because given k,Signsk​(k),Mack​(M) an attacker can forge k,Signsk​(k),Mack​(M′) on any M′ of its choice.**

Let G be a group, and consider the following private-key encryption scheme with message space G: The shared key is a uniform element k∈G. To encrypt a message m∈G using key k, output the ciphertext k⋅m. To decrypt a ciphertext c∈G using key k, output the message k^−1 \* c. Which of the following is true about this scheme?

**- The scheme is perfectly secret.**

Consider hybrid encryption using plain RSA and AES-128 in CTR mode, with public key N,e. Say a 128-bit message m is encrypted, yielding ciphertext c,c0​,c1​, with c∈ZN∗​ and c0​,c1​∈{0,1}128. Which of the following would be an encryption of mˉ, the bitwise complement of m?

**- c,c0​,cˉ1​.**

Say El Gamal encryption is used in the subgroup of Z47∗​ generated by 4. The public key is 21 and the private key is 4. The ciphertext (34,42) is an encryption of some message m. Which of the following is an encryption of [4m mod47]?

**- (34, 27)**

Consider the plain RSA encryption scheme with public key N=55,e=3. Say the encryption of some unknown message m is 6. What is the encryption of [2m modN]?

**- 48**

Say you have "oracle access" to a piece of code that, given a message m, appends an unknown 8-byte password p, applies PKCS #7 padding, and then encrypts the result using AES-128 in ECB mode with an unknown key. Which of the following attacks can be used to confirm that the first byte of p is 'Z'?

**- Submit the 15-byte message "ABCDEFGHIJKLMNO" and the 16-byte message "ABCDEFGHIJKLMNOZ," and check if the first blocks of the resulting ciphertexts are equal.**

**Hardware security**

**Week-1**

**1.**

Вопрос 1

As her Christmas gift, Joyce received a toy doll with a small computer chip embedded. When she presses the tummy of the doll, it says "Hello, Joyce!"; when she presses again, it says "Merry Christmas!"; on the next press, it says "I love you!"; and whenever Joyce presses twice quickly, it says "Good-bye!".

Which of the following statements about the doll are correct? Check all that apply.

the chip can recongize two different inputs

the chip contains memory elements

**2.**

Вопрос 2

Bob is designing a digital system to implement the multiplication table. When two single-digit integers (0-9), e.g. 4 and 7, are entered, the system will output their product (28 in this case). When both input and output are expressed in binary, the system should have 8 bits as input (4 bits for each number) and 7 bits as output (the largest output is 81 and needs no more than 7 bits).

There are 2^8 = 256 combinations for the 8 input bits. However, for the multiplication table, there will be only 100 entries (axb with both a and b go from 0 to 9). So there will be 256-100 = 156 don't care conditions.

Please enter 1 to show that you have understood this and earn the point :)

1

**3.**

Вопрос 3

Which of the following gate(s) are universal? Check all that apply.

hint: A universal gate should be able to implement {AND, OR, NOT}

NAND

{OR, NOT}

Вопрос 4

For the 3-input gate *f*(*x*,*y*,*z*)=*x*’*yz*+*xy*’+*y*’*z*, what is the value of *f*(*x*,0,1)?

1

**5.**

Вопрос 5

*f*(*x*,*y*,*z*) is a 3-input 2-output function. How many different *f*(*x*,*y*,*z*) can we have to make *f*(0,0,1)=01,*f*(0,1,0)=10,*f*(1,0,0)=11 ?

(hint: Two functions are different if there is an input combination on which the two functions give different output. Think about what could be the output of �*f* on each of the input combinations other than the 3 specified cases).

1024

**6.**

Вопрос 6

For the four 2-input logic gates (NAND, NOR, XOR, XNOR), each with x and y as their inputs, which of the following statements about observability don't care (ODC) are true? Check all that apply. (If you forget the definition of these standard logic gates, you can find them in the slide "Example: System Implementation").

there is no ODC for XNOR gate

when y=0, x input is ODC for NAND gate

**7.**

Вопрос 7

Consider the following two functions, S and C, defined on three inputs x, y, z: *S*(*x*,*y*,*z*)=*x*⊕*y*⊕*z*, *C*(*x*,*y*,*z*)=*x*∙*y*+*z*∙(*x*⊕*y*), where ⊕⊕ is the XOR gate, ++ is the OR gate, and ∙∙ is the AND gate.

Which of the following conditions are satisfiability don't cares? Check all that apply.

x=0, z=0, C=1

x=0, y=0, z=1, S=0

**Week-2**

**1.**

Вопрос 1

Which of the followings are the goals of IP protection? Check all that apply.

Trace IPs

Protect IP against unauthorized use

Protect testing data associated with the IP

**2.**

Вопрос 2

You want to minimize a 4-variable function *F*(*a*,*b*,*c*,*d*) with two don't care conditions, {*a*=*b*=*c*=*d*=1} and { *a*=*d*=1,*b*=*c*=0} (or *abcd* and *ab*′*c*′*d*). To embed your signature with the watermarking approach described on slide "Watermarking a Boolean Formula" (page 1 in "Watermarking Examples"), you decide to minimize *F*(*a*,*b*,*c*,*d*)+*abcd* instead, what is your signature?

10

**3.**

Вопрос 3

A good watermark will be difficult or impossible to be removed by any adversary without detailed knowledge about the watermark, this property is known as

Resilience

**4.**

Вопрос 4

A good watermark should not require major modification to the industrial design tools and design software, this property is known as

Transparency

**5.**

Вопрос 5

In the slide of "Public Watermarking GP Problem" (page 6 in "Good Watermarks"), which of the followings should be made to the public? Check all that apply.

The pairs of nodes selected to embed the public watermark bits

The scheme that public watermark head and body will be constructed

The public watermark you want to embed in the solution

The rules on how each public watermarking bit will be embedded

**6.**

Вопрос 6

In the node duplication example for fingerprinting graph coloring solutions, (see slide "Fingerprinting: Node Duplication", page 4 in "Fingerprinting"), if we add a new node B' as the duplicate of node B, which nodes should B' be connected to? Check all that apply.

ABCD

**7.**

Вопрос 7

Bob decides to use the clique manipulation method to generate fingerprinting solutions to the graph coloring problem, (see slide "Fingerprinting: Clique Manipulation", page 5 in "Fingerprinting"). He finds a clique of 4 nodes and apply the method. How many distinct solutions can Bob generate?

4!=24

**8.**

Вопрос 8

In the slide "Fingerprinting: Don’t Cares (I)" (page 6 in "Fingerprinting"), Alice decides to create fingerprinting copies of the original circuit by adding a new connection to the OR gate, which of the followings are correct? Check all that apply.

Connect signal X’ to the OR gate

**9.**

Вопрос 9

When we use serial number as the tag for a device, which property does this tag have? Check all that apply.

reproducible

passive

**10.**

Вопрос 10

IC metering methods that can also be used to lock, unlock, enable, disable, or controll the IC are known as \_\_\_\_\_\_\_\_ metering method.

active

**11.**

Вопрос 11

IC tags that are based on fabrication variations have the property of \_\_\_\_\_\_\_\_\_\_\_\_ and therefore will be a good candidate to countermeasure foundry overbuilding.

Unclonable

**Week-3**

**1.**

Вопрос 1

Which of the followings about physical attacks is *incorrect*​?

All physical attacks will make damage to the system

**2.**

Вопрос 2

Which of the following physical attacks is invasive?

Microprobing

**3.**

Вопрос 3

Which of the following non-invasive attacks is passive?

Side channel attack

**4.**

Вопрос 4

Which of the following about invasive attacks is true?

It is possible to probe into a single bus line and inject data to control bus activity.

**5.**

Вопрос 5

Which of the following statements is true for data remanence on SRAM?

It is possible to freeze data and read it at temperature higher than -20 degree.

**6.**

Вопрос 6

When we use the "iterative exponentiation and modular" method to compute 24(*mod* 5), starting from 2121, we will have 21=2(*mod* 5); 2×2=4(*mod* 5); 4×2=3(*mod* 5); 3×2=1(*mod* 5). The results we will see are 2, 4, 3, 1. If we use the same method to compute 37(*mod* 5), starting from 3131, the results we will see are

3,4,2,1,3,4,2

**7.**

Вопрос 7

Which of the following decimal to binary conversion is *incorrect*​?

37=101011

207=11110011

**8.**

Вопрос 8

For e=1001010110, when we compute *ae*(*mod* *n*) with the left to right "square and multiple algorithm (I)", the total number of multiplication (both b\*b and b\*a) we will do is

15

**9.**

Вопрос 9

In the slide of "Montgomery Reduction", which one of the following conditions is necessary?

gcd (R,N) = 1

**10.**

Вопрос 10

The Montgomery reduction of 25 modulo 109 w.r.t. 128 is (just enter your answer, for example, 6)

30

**Week-4**

**1.**

Вопрос 1

True or false: In all side channel attacks, the attacker must have physical access to the system under attack to collect side channel information.

False

**2.**

Вопрос 2

True or false: Side channel attacks are passive, but they can be combined with active attacking methods to become more effective in breaking the system.

True

**3.**

Вопрос 3

True or false: The power and delay of different instructions are normally different.

True

**4.**

Вопрос 4

True or false: The power and delay of the same instruction on different oprands can also be different.

True

**5.**

Вопрос 5

True or false: The optical side channel attacks are rare because they require expensive equipment.

False

**6.**

Вопрос 6

True or false: Hitting different keys or key combinations on the keyboard will generate different acoustic traces. This can leak side channel information

True

**7.**

Вопрос 7

True or false: When the secret data stored in cache or register is overwritten by other data, this memory load (or data overwriting) operation will not leak any information about the secret data.

False

**8.**

Вопрос 8

True or false: When the cache storing secret data is shared by other processes, it may introduce security vulnerabilities.

True

**9.**

Вопрос 9

Which of the following, according to Kocher's 1996 paper, is not necessary to launch a successful timing attack?

All of the above are necessary

**10.**

Вопрос 10

Which of the following statements about differential power analysis (DPA) is true?

DPA needs tools or skills to analyze the power traces

**11.**

Вопрос 11

Both Kocher's and Schindler's timing attacks can break RSA algorithm. Which of the following statements is true?

Kocher's timing attack targets the RSA decryption key.

**12.**

Вопрос 12

The following actions can form a scan chain based attack on a system with 5 flip flops.

What is the correct order to launch the attack?

A. set TC=0, let the system run for one clock cycle.

B. set TC=1, read the output from scan out for 5 cycles.

C. set TC=1, send state information to the system via scan in for 5 cycles.

D. set TC=0, apply the input value at the system's primary input ports.

CDAB

**13.**

Вопрос 13

Which of the followings will not help to prevent side channel attacks?

Use sensor mesh at the top metal layer and continuously monitor all paths in the mesh.

**14.**

Вопрос 14

�(2015)=‾*ϕ*(2015)=​ (hint: factor 2015 to primes)

1440

**15.**

Вопрос 15

Which of the following statements about the randomized modular exponentiation (ME) is true?

The random number *r*2​ cannot be 0.

**Week-5**

**1.**

Вопрос 1

Which of the followings added by a system designer will be considered as a hardware Trojan?

Use an additional signal to write the plain text to memory before it goes into the encryption block.

**2.**

Вопрос 2

In the example we have showed for trusted IC and hardware Trojan, the following functions are used to implement �(�)=�2*F*(*x*)=*x*2:

�1=�1*Z*1​=*X*1​

�2=�2�3*Z*2​=*X*2​*X*3​

�3=(�1+�2)�4+�2�3′*Z*3​=(*X*1​+*X*2​)*X*4​+*X*2​*X*3′​

�4=(�2⊕�3)�4*Z*4​=(*X*2​⊕*X*3​)*X*4​

�5=�3�4′*Z*5​=*X*3​*X*4′​

�6=0*Z*6​=0

�7=�4*Z*7​=*X*4​

what will be the output when 11102=141011102​=1410​ is entered as the input? Enter your answer in binary and from �1*Z*1​ to �7*Z*7​.

1100100

**3.**

Вопрос 3

We have shown that replacing �2=�2�3*Z*2​=*X*2​*X*3​ with �2=(�1+�2)�3*Z*2​=(*X*1​+*X*2​)*X*3​ will add a hardware Trojan to the circuit in question 2. Which of the following statements about hardware Trojan-free (or trusted IC) implementation is FALSE?

Replacing �6=0*Z*6​=0 by �6=�1�3*Z*6​=*X*1​*X*3​ cannot prevent the hardware Trojan showed in this question.

**4.**

Вопрос 4

Hardware Trojans can be functional, which will change the system's functionality, or non-functional, which do not. Non-functional hardware Trojans are also known as \_\_\_\_\_\_\_\_\_ Trojans.

Parametric

**5.**

Вопрос 5

Which of the following statements about hardware Trojan detection is true (assume that the Trojan detection tool is trusted)?

When a Trojan is reported, the IC cannot be trusted.

**6.**

Вопрос 6

Which of the following statements about physical attacks and hardware Trojan detection approaches is FALSE?

Physical attacks can be invasive, but hardware Trojan detection cannot.

**7.**

Вопрос 7

Which of the following statement about side channel analysis based hardware Trojan detection methods is INCORRECT?

The errors in collecting side channel measurements do not impact the accuracy of these detection methods.

**8.**

Вопрос 8

A small kill switch (a 2-input AND gate and a triggering signal) is added to the chip to disable the encryption engine. Which of the following hardware Trojan detection approaches most likely will NOT be able to catch it?

Power side channel analysis

**9.**

Вопрос 9

For two FSMs M1 and M2 and their product machine M, which of the following statements about FSM equivalence is correct?

If M1 and M2 give different outputs for the following input 1010101010, they cannot be equivalent.

**10.**

Вопрос 10

Which of the following statements about hardware Trojan prevention is true?

Shadow registers can help to measure the delay of internal paths. So it can make the path delay based hardware Trojan detection approaches more effective.

**11.**

Вопрос 11

Which phase in the IC supply chain is considered trusted?

Specification

Deploy and monitor

**12.**

Вопрос 12

Which of the following is NOT a payload of hardware Trojan?

Remove IC designer's watermark

**13.**

Вопрос 13

Which of the following hardware Trojan detection methods CANNOT catch non-functional Trojans?

Logic test based approaches

**14.**

Вопрос 14

Which of the following approaches is a pre-synthesis hardware Trojan prevention method?

Test and validation

Formal verification

**Week-6**

**1.**

Вопрос 1

True of false: the endorsement key in TPM is a non-migratable key.

True

**2.**

Вопрос 2

True of false: if the user provides the same password to different TPM chips, the same storage root key will be created.

False

**3.**

Вопрос 3

True of false: all the TPM migratable keys are generated outside the TPM and thus they cannot be trusted.

False

**4.**

Вопрос 4

Which of the followings are functions of TPM? Check all that apply.

store user passwords, encryption keys and digital certificates

generate and store cryptographic keys

generate pseudo-random numbers

**5.**

Вопрос 5

Which of the following PUFs are memory based. Check all that apply.

Butterfly PUF

SRAM PUF

**6.**

Вопрос 6

Which of the following methods can make the RO PUF more reliable? Check all that apply.

Use error correction coding to correct the PUF bit flips.

Run the RO pairs for a longer time.

**7.**

Вопрос 7

Which of the following features make the configurable RO PUF reliable? Check all that apply

Inverters that are sensitive to temperature or supply voltage can be excluded.

The configuration vector is selected after the chip is fabricated

**8.**

Вопрос 8

Which of the followings need to be considered when a true random number generator (TRNG) is evaluated? Check all that apply.

power efficiency of the TRNG

the source of entropy for the TRNG

complexity of implementing the TRNG

**9.**

Вопрос 9

When an FPGA system developer detects a hardware Trojan from the FPGA chip he has purchased, where the hardware Trojan may come from? Check all that apply.

FPGA vendor who designed the FPGA chip

IP vendor whose IP is included in the FPGA chip

Foundry that fabricates the FPGA chip

EDA tool vendor whose design tool is integrated in the FPGA design environment

**10.**

Вопрос 10

When Bob purchases an FPGA-based system, which of the following security vulnerabilities and attacks he should consider. Check all that apply.

Hardware Trojan inside the FPGA-based system

User's sensitive information leaking from the system

**Week-7**

**1.**

Вопрос 1

True or false: On a sequential system, to control the accessibility of a state �*u*, it is sufficient to check all the transitions �→�*v*→*u* for the starting state �*v* and the transition condition.

False

**2.**

Вопрос 2

A system is supposed to output 1010 on input 00011010, but outputs 0101 after a digital watermark is embedded. Which requirement does this watermarking method violate?

Correct Functionality

**3.**

Вопрос 3

Which of the followings are the goals of IP protection? Check all that apply.

Protect IP against unauthorized use

Enable the IP owner to detect the use of the IP

Protect testing data associated with the IP

**4.**

Вопрос 4

When we use ICID as the tag for a device, which property does this tag have?

passive

**5.**

Вопрос 5

Convert the decimal number 2015 into binary: (write the binary number only, for example: 10101010101. No space, comma, etc.)

11111011111

**6.**

Вопрос 6

Which of the following PUFs are delay based? Check all that apply.

Ring Oscillator PUF

Arbiter PUF

**7.**

Вопрос 7

Which of the following statements about digital watermarking and fingerprinting is correct?

A fingerprinting method has to guarantee that different copies of the same IP get different fingerprints.

**8.**

Вопрос 8

Which of the following statements about don't care conditions is correct?

When a combinational system is fabricated, the outputs will be deterministic for all the don't care conditions, but outputs may have different values on different don't care conditions.

**9.**

Вопрос 9

Which of the following statements about physical attacks is correct?

All physical attacks will need the help from some tools and/or equipment.

**10.**

Вопрос 10

Which of the followings can be used to generate fault for fault injection attacks to a system?

All of the above

**11.**

Вопрос 11

Which of the followings is NOT a good practice in securing a system?

design a working system and then add the necessary protocols to secure it

**12.**

Вопрос 12

Which of the following statements about side channel attacks is NOT correct?

All side channel attacks need direct access to the system to collect side channel information.

**13.**

Вопрос 13

Which of the followings can be potential sources for side channel attacks? Check all that apply.

system's output signals

electromagnetic radiation

power consumption

system's timing or delay information

acoustic side channel

scan chain output signals

optical side channel

**14.**

Вопрос 14

Consider *w*=*x*’*yz*+*xy*’+*y*’*z*, which of the following conditions is a satisfiability don't cares?

*x*=1,*y*=0,*w*=0

**15.**

Вопрос 15

When an FSM is implemented, which of the followings will be considered as a hardware Trojan?

Connecting the FSM to an antenna to send out the FSM state information.

**16.**

Вопрос 16

For an FPGA-based system developer, which of the following security vulnerabilities and attacks he will not care?

Watermarks in the FPGA embedded by the FPGA vendor.

**17.**

Вопрос 17

The following 4 questions are on how to use Montgomery Reduction method to compute 67×58(*mod* 109). Here we have  *a*=67,*b*=58,*N*=109. We pick *R*=128 and we know that *N*−1=101(*mod* 128).

What is *a*′=*aR*(*mod* 109)? Write the number only, no need to append (*mod* 109).

74

**18.**

Вопрос 18

Continue from the previous question, what is *b*′=*bR*(*mod* 109)?

12

**19.**

Вопрос 19

Continue from the previous question, what is *c*′=(*a*′*b*′)*R*−1(*mod* 109)?

41

**20.**

Вопрос 20

Continue from the previous question, what is *c*=*ab*(*mod* 109)?

71

**21.**

Вопрос 21

What is the modular multiplicative inverse of 5(*mod* 38)?

(hint: use Euler's Theorem, square and multiply).

23