Corrected

EPFL

1

Teacher: Prof. Dr. ETH Mathias Payer
COM-402 Information Security and Privacy – Quiz 03
25th November 2024
Duration: 15 minutes

Anon Ymous

SCIPER : **999999**

Do not turn the page before the start of the quiz. This document is double-sided, has 4 pages, the last ones possibly blank. Do not unstaple.

- **No other paper materials** are allowed to be used during the quiz.
- Using a **calculator** or any electronic device is not permitted during the quiz.
- For each question, mark the box(es) corresponding to the correct answer(s). Each question has **one or more** correct answers.
- For each question, we give:
  3 points by default,
  0 points if you give no answer,
  −1 point per incorrectly checked or missed answer.
  Each question has a minimum of 0 points, we do not award negative points.
- Use a **black or dark blue ballpen** and clearly erase with **correction fluid** if necessary.
- If a question is wrong, we may decide to nullify it.

Respectez les consignes suivantes | Observe this guidelines | Beachten Sie bitte die unten stehenden Richtlinien		
choisir une réponse | select an answer Antwort auswählen	ne PAS choisir une réponse | NOT select an answer NICHT Antwort auswählen	Corriger une réponse | Correct an answer Antwort korrigieren
☒ ☑ ■	☐	☐ ▭
ce qu'il ne faut **PAS** faire | what should **NOT** be done | was man **NICHT** tun sollte		
▨ ☒ ▢ ▪ ▨ ▢		

Corrected

Question 1
According to a paper by Böhme and Falk, the time required to discover the same coverage scales *linearly* with the number of machines used when discovering the same bugs, but *exponentially* when discovering *new* bugs. Select all the correct implications of this statement.

- [ ] If your fuzzing campaign reached 50% coverage, you need twice the compute power to reach the same coverage in half the time.
- [ ] If your fuzzing campaign reached 50% coverage, you need twice the compute power to reach the same coverage in double the time.
- [ ] There will be some bugs fuzzers won't discover.
- [ ] If your fuzzing campaign reached 50% coverage, you need twice the compute power to reach double the coverage in double the time.

Explanation: As the number of machines used in a fuzzing campaign increases, the time to discover new bugs grows exponentially. Furthermore, some "deep" bugs (e.g., masked behind cryptography routines) are going to be very hard to be discovered by fuzzers.

Question 2 Which of the following statement(s) is/are true about Android and its security?

- [ ] Source code of Android is made available through the Android Open Source Project (AOSP). Vendors (OEMs) may customize AOSP code to their specific hardware.
- [ ] Security bugs found in AOSP are patched by Google, and later published through the Monthly Security Bulletin.
- [ ] An important security challenge of Android devices is fragmentation, i.e., many different Android versions and customizations.
- [ ] Like Android, iOS maintains an open ecosystem, and similarly suffers from fragmentation issues.

Explanation: In contrast to Android, iOS has a very closed ecosystem. iOS is not open source and Apple is the only manufacturer of iDevices, which rollout iOS updates consistently.

Question 3
What is the correct definition of `Activity` in the Android.

- [ ] It performs an action in the background with a specified interval.
- [ ] It's the entry point for interacting with the users and Activities generally define UIs.
- [ ] It responds to system-wide events such as when an SMS is received.
- [ ] It provides shared interface for app data which other applications can query or interact.

Explanation: `Service` performs an action in the background with a specified interval. `Broadcast receiver` responds to system-wide events such as when an SMS is received. `Content provider` provides shared interface for app data which other applications can query or interact.

CORRECTED

Question 4

Anti-Fuzz is a technique proposed to protect released binaries from being fuzzed. The attack model of the technique is that adversaries can only access the protected binaries (with obfuscations), and the protected binaries are difficult to fuzz. Only the original developers have access to the source code and therefore can find/fix bugs faster than the attacker. For this technique, which statement(s) is/are correct?

- ☐ Attackers can only do black-box fuzzing on the protected binary as they don't have source code.
- ☐ This technique can be used to protect the Linux kernel.
- ☐ One possible way to obfuscate (protect) the binary is to slow down its execution speed.
- ☐ Anti-fuzz hardens the binaries so that bugs can no longer be exploited.
- ☐ Anti-Fuzz is a kind of compartmentalization technique.

Explanation: A) Greybox fuzzer can use QEMU or Intel-Pin to get coverage for binaries that do not have coverage instrumentation. B) The attack model is that adversaries would not have access to source code. While the Linux kernel is open source, the attack model does not hold D) Anti-Fuzz should not change program behavior. The bug exists in original code still persists in the anti-fuzz harden binary. E) Anti-Fuzz does not compartmentalize the programs into components; it's more like program confusion.

Question 5

Which of the following statement(s) is/are true about software testing?

- ☐ Covering 100% of the target program's code indicates that fuzzing is complete.
- ☐ Covering 100% of the target program's input space indicates that fuzzing is complete.
- ☐ Static analysis is incomplete due to the lack of runtime information.
- ☐ Symbolic execution is incomplete due to state explosion, but sound.

Explanation: Covering 100% of the target program's code does not indicate the fuzzing is complete, because some bugs require satisfying certain data-flow restrictions to trigger.

CORRECTED

Question 6
Which of the following statement(s) about network security is/are true?

- [ ] Confidential resources should be accessible in the DMZ directly
- [ ] A standard ring network architecture is as secure as a segmented network.
- [ ] Virtual LANs (VLANs) allow for distinct devices to be perceived as part of the same network. It is therefore a compartmentalization strategy.
- [ ] Zero Trust Networks reduce the impact of compromised devices by assuming no one/nothing is to be trusted, not even internal machines' communication

Explanation:

- DMZs allow access to certain pre-defined resources to all the network. It is used to provide external-facing services (like a mail service or webstite). As such, sensitive information should not be accessible in the DMZ.
- Ring networks do not adhere to the principle of least privilege: a person who needs access to a service in a given ring will also have access to all other services in that ring. Segmented networks enforce a (firewall) rule-based access per service.
- VLANs are configured at the switch level (level 2) which allows to virtually segregate machines into different zones, which by definition, is a form of compartmentalization. (In modern switches, VLANs can also cross the physical switch boundary, further enhancing their comparmentalization ability)
- ZTNs: this is the deifnition of a Zero Trust Network.

Question 7
Which of the following statement(s) about sanitizers is/are true?

- [ ] If a program is compiled with sanitizers, all bugs of the bug class covered by the sanitizer will be reported at compile time.
- [ ] If a program is compiled with sanitizers, all bugs of the bug class covered by the sanitizer will be reported at run time.
- [ ] Sanitizers are useful for fuzzing because they can serve as a bug oracle.
- [ ] Some sanitizers (e.g., ASAN) can be applied to both source code and binary-only software.

Explanation:

- Sanitizers detect bugs at run time, not at compile time.
- Only bugs that are in the concrete execution path can be detected. More specifically, all bugs in control flow paths that are not executed will not be reported by the sanitizer.
- Sanitizers enforce aborts/crashes when they detect a violation and therefore serve as a bug oracle during fuzzing.
- Some sanitizers, e.g., ASAN, can be applied via instrumentation in the compiler toolchain as well as through binary instrumentation (see, e.g., QASAN, valgrind, RetroWrite, ARMore, ...)

CORRECTED

Question 8
Android...

- [ ] ... can be built and flashed to a device by yourself because of the AOSP.
- [ ] ... is based on the same kernel as iOS and just provides a different user space runtime and runtime API to apps.
- [ ] ... is based on the same kernel as Linux distributions such as Ubuntu.
- [ ] ... can install Ubuntu packages and run arbitrary Linux binaries unmodified.

Explanation:

- Manufacturers add device-specific binary firmware blobs and other customizations that are not part of the AOSP and usually hard to obtain for end users.
- Android is based on the Linux kernel, whereas iOS is based on Apple's XNU kernel.
- Android is based on the Linux kernel and therefore shares its underlying basis with desktop or server Linux distributions.
- While Android is based on Linux, it cannot run arbitrary Linux binaries out of the box due to missing/different libraries, IPC mechanisms, user space runtime restrictions, etc.

Question 9
As CISO you worry about hackers who exploit browser vulnerabilities (by luring employees to dubious websites) and then escalate privileges to fully compromise your employees' workstations. Which of the following security measures apply to this scenario and will either prevent or make such attacks more difficult? strategy

- [ ] Keep the operating systems and all software up-to-date.
- [ ] Encrypt the hard drive.
- [ ] Configure the workstations to disable JavaScript in installed browsers.
- [ ] Configure the workstations such that the only browser employees can use is Internet Explorer

Explanation:

- If the OS is outdated when such attackers escalate privileges there are potentially n-days that may be exploited
- Does not apply to this particular attack scenario (relevant for physical attacks)
- JavaScript is a huge attack surface in browsers, disabling JavaScript shrinks the attack surface -> makes such attacks harder
- Internet Explorer can have vulnerabilities (also not supported anymore etc..)

CORRECTED

Question 10
Which of the following is/are true for VPNs?

- [ ] VPNs and VLANs both describe virtual networks and are therefore synonymous terms.
- [ ] VPNs fully anonymize a user browsing the web by masking the user's IP address.
- [ ] VPNs generally encrypt the tunneled traffic but can also operate without encryption.
- [ ] Depending on the implementation, VPNs can tunnel traffic both Ethernet and IP traffic.

Explanation:

- VPNs bridge networks, VLANs segment local networks.
- VPNs mask the user's IP address but the user might still be identified through other measures such as cookies in the browser or browser fingerprinting.
- VPNs commonly encrypt tunneled traffic but some VPN VPN implementations can tunnel traffic without encryption, e.g., IPSec.
- It is possible for VPNs to tunnel IP traffic only (which is the most common use case) but implementations such as L2TP allow tunneling link layer traffic to make devices seem to be on the same local link.

Question 11
Which of the following is/are true for proxies?

- [ ] Proxies operates at the network layer.
- [ ] Direct proxies protect users when they access servers on the Internet.
- [ ] Reverse proxies protect servers when accessed by users from the Internet.
- [ ] Web Application Firewall is a type of direct proxies.
- [ ] Mail gateways act both as direct proxy and reverse proxy.

Explanation:

- Proxies operates at the application level.
- These are the definitions of direct proxies and reverse proxies.
- Web Application Firewall is a type of reverse proxies with the goal of protecting a web server against malicious requests from the Internet.
- All outgoing mail is stored on the mail gateway before being forwarded to the internet and all incoming mail is intercepted by the gateway before being forwarded to the users' mailbox. So it acts as both proxy and reverse proxy.