

Question 1. Possible attack scenarios

a) Main-in-the-middle attack

Main-in-the-middle attack is the case where a client is in mind that one is communicating with the company service but is actually communicating to the service via a third-party mediator. For example, if an attacker alerts a user that one needs some action within University-C137 money transfer system with a link to a phishing website of the system, the subject will leak ones access information by logging into the phishing website.

In such scenario, this results in a compromised confidentiality, and the user may end up in financial losses.

b) Side channel attack

A possible side channel attack would include a reflection of personal information. A user may utilize company's money transfer service not knowing that one's monitor is being watched from behind or through reflection of nearby object surface.

This will result in compromised confidentiality, as this leaks personal information, or even authentication information to the attacker.

c) Privilege escalation

A possible privilege escalation attack may be done by buffer overflow attack. The attacker conduct fuzzing on company service, and detect buffer overflows, which then can be used to replace existing program instructions with desirable ones.

At worst case, the attacker can get their hands on the root privilege, which violates confidentiality and possibly integrity and availability as the attacker has full control over the device that runs the service.

Question 2. Approaches to conduct each phase of development

Code review

- I would suggest with guided code reviews rather than using techniques like "easter egg" code reviews as the service hasn't been maintained properly for a long time, it is expected to have a lot of side effects to begin with. The code review will be done per each change of features made by individual developers. The developers will have a meeting and explain, cooperatively inspect the algorithm and codes to find flaws or better approach to the problem before it can be merged to communal branch.

Testing

- The service must conduct white-box regression testing on each update to check two things: make sure the service does what it is supposed to do; make sure the service does not do what it is not supposed to do.
- For each new features, it must come with unit tests that inspects of above two categories.
- Every update must pass all unit tests of the module before it can be pushed in

Maintenance

- Code reviews and testing are not a one-time job. In order to limit the number of flaws, product development must be formalized with establishment of standards and audits.
- Development process will follow 5 step sprint agile principle; sprints with 5 phases: planning, implementation, review, deployment, retrospective. Each sprint will be 2 weeks long. Code review and testing are done under review phase.
- Audits from external organization would be preferable but having such audit maybe costly and not always accessible. Thus, the company will allow audits of development procedure by supervisors of each department. For each development cycle, audits need to submit a development guideline checklist based on agile principle, preferably with comments on potential improvements or explanations on unsatisfied entries.

Question 3. Reinforce the defense mechanisms.

present how they could be used to defend against any one of the attacks mentioned

provide one attack from question 1 as an example

- Prevent. In case of a Side channel attack, the service can authenticate user using biometrics so that reflections of the scree no longer reveal user's authentication information.
- Deter. In case of a Privilege escalation, the service can use virtual memory mapped to randomized physical addresses so that exploiting buffer overflow vulnerability to act as desired behavior is difficult.
- Deflect. In case of any attack methods above, the service can have a limit on the amount money one can transfer at a time and day. In this case, the attacker will find the service as less attractive target since they would not be profited much even if they successfully exploit the service.
- Detect. In case of stolen authentication from Main-in-the-middle attack, the exploit can be detected by sending a confirmation message to the user that a login from a new device is detected.
- Recover. In case of system corruption after the attacker exploited privilege escalation, the service can be recovered by having a backup image of service data on remote drive.

Question 4.

a) 3 times for authentication chances is small enough that user will often be locked out of their own device by accident. Also, password based single factor authentication is vulnerable as there are numerous ways for the attacker to get their hands on user's passwords

b) 2FA with more authentication chances will prevent from getting accidentally locked out of one's own device. Furthermore, it would make more difficult to exploit the device as the attacker needs to obtain both of the authentication keys to login as the user.

Question 5. Malware analysis

a) CryptoLocker

type: ransomware or scareware

infection: spoofed e-mail attachments from a botnet

effect: Encrypted victim's hard drive

b) Stuxnet

type: worm

infection: 4 different zero-day attacks or manual installation via USB drive

effect: subtly changes the frequencies of installed variable-frequency drives operating between 807–1210 Hz so that

distortion and vibrations occur resulting in broken centrifuges.

c) CIH

type: virus

infection: spread using executable files, infecting other executable files

effect: DoS on victim device by corrupting BIOS