Security questions check-list
Security

R. Absil

Academic year 2024-2025

The following document provides a check-list of several security features that most likely should be implemented in any distributed application, whether they are desktop, web or mobile. It is important to be able to answer all these questions, even if the answer means there is a vulnerability.

If you answer a question stating your are not vulnerable to a particular risk, you have to be able to detail the features you implemented that allows you to fight attacks related to this risk. On the other hand, should you be vulnerable to a particular risk, you have to detail the potential features you implemented to slow down attacks and mitigate their effects, as well as what you could to to prevent this type of risks.

Check-list

1. Do I properly ensure confidentiality?
    - Are sensitive data transmitted and stored properly?
    - Are sensitive requests sent to the server transmitted securely?
    - Does a system administrator have the ability to access any sensitive data?
2. Did I harden my authentication scheme?
    - Do I use Captcha, MFA, a zero-knowledge proof scheme?
3. Do I properly ensure integrity of stored data?
4. Do I properly ensure the integrity of sequences of items?
    - Does somebody has the ability to add or delete an item in a sequence, or edit an item in a sequence, without being detected?
5. Do I properly ensure non-repudiation?
6. Do my security features rely on secrecy, beyond cryptographic keys and access codes?
7. Am I vulnerable to injection?

- URL, SQL, Javascript and dedicated parser injections

8. Am I vulnerable to data remanence attacks?
9. Am I vulnerable to fraudulent request forgery?
10. Am I monitoring enough user activity so that I can detect malicious intents, or analyse an attack *a posteriori*?
    - Am I properly sanitising user input?
    - Did I implement some form of anomaly detection?
    - Do I use a whistleblower client?
11. Am I using components with know vulnerabilities?
12. Is my system updated?
13. Is my access control broken (cf. OWASP 10)?
14. Is my authentication broken (cf. OWASP 10)?
15. Are my general security features misconfigured (cf. OWASP 10)?