Initial Post

◄ Initial Post

Display replies in nested form

Settings

Initial Post

by Anda Ziemele - Sunday, 27 October 2024, 4:28 PM

I have selected Cryptographic Failures, holding the position of number two in the OWASP Top 10 identified weakness (OWASP, 2021). The flowchart of processes and decisions is presented in Figure 1.

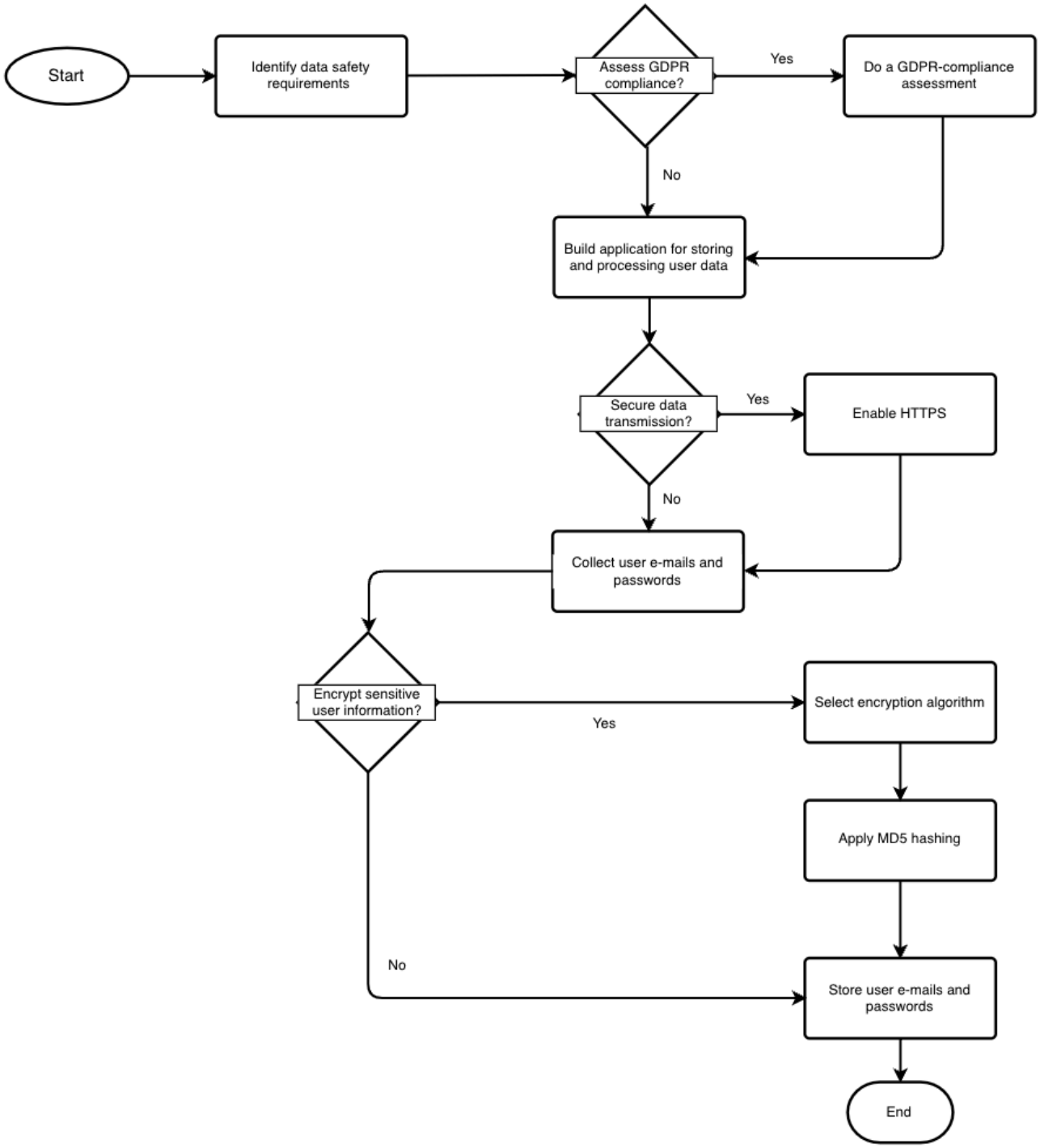

Figure 1. Flowchart of introducing a subset of cryptographic failures.

Following the phase of SDLC, the first stage, Planning stage, considers the project requirements. Here, insufficient assessment of what data needs to be encrypted and secured, and the strength at which it needs to be secured, can lead to weak software security designs. Additionally, depending on where the data is processed, additional GDPR compliance measures may apply, including the requirement of sufficient systems and data securement (Allen, 2023). An incomplete assessment or failing to assess GDPR compliance of designed systems can lead to heavy fines and reputation loss.

When designing the application, there are critical decisions pertaining to security. Firstly, when transmitting data, a secure internet protocol such as HTTPS must be implemented to transmit sensitive data. Failure to do so can result in interception by malicious actors. Following this, any data stored must be encrypted and a sufficiently secure encryption algorithm must be selected. For example, MD5 hashing algorithm, although fast, is vulnerable to brute-force and collision attacks (Stec, 2024). SHA256 however currently has no known vulnerabilities.

In conclusion, cryptographic failures can occur at all stages of software design and development, with most critical decisions pertaining to encrypting data when processing, storing and retrieving. When designing software, a thorough assessment should be done to ensure the application is fully secure and compliant with the relevant security standards (GDPR, and also PCI-DSS, for example).

References:

Allen, C. (2023) Encryption For GDPR Compliance. *Cryptomathic*. Available from: **https://www.cryptomathic.com/blog/encryption-for-gdpr-compliance** [Accessed 27 October 2024]

OWASP (2021) OWASP Top 10. *OWASP*. Available from: **https://owasp.org/www-project-top-ten/** [Accessed 25 October 2024]

Stec, A. (2024) MD5 vs. SHA Algorithms. *Baeldung*. Available from: **https://www.baeldung.com/cs/md5-vs-sha-algorithms** [Accessed 27 October 2024]

Permalink **Reply**

Re: Initial Post

by Cathryn Peoples - Sunday, 27 October 2024, 7:56 PM

Hi Anda,

Thank you very much for initiating Collaborative Discussion 1.

You might decide on including an introduction into your post, which could involve explaining what cryptographic failures are.

In relation to the 1st process, 'Identify data safety requirements', I would like to know where. Where are data safety requirements being assessed?

I would rename the first decision as 'GDPR compliance?', with Yes and No paths leaving the decision node. It is perhaps unnecessary to have a 'Do a GDPR-compliance assessment' - I'm assuming that the output of this process would already be known when exiting the first decision node.

It's not obvious to me why 'Secure data transmission?' is included after 'Build application ...' Isn't securing the data transmission part of the process of building the application?

Under which conditions would a decision be made to 'Encrypt sensitive information'? It's not clear to me where and when such as decision would be made. What type of application are you considering?

Good use of referencing. Remember that in academic writing, we define all acronyms when they are first used in your writing, followed by the acronym in brackets. The acronym can then be used from this point onwards e.g., General Data Protection Regulation (GDPR).

Hope that helps.

Cathryn

Permalink **Show parent** **Reply**

Peer Response

by Andrius Busilas - Thursday, 31 October 2024, 5:32 PM

Hi Anda,

"Cryptographic Failures," a crucial aspect of secure software development, holds a significant position in the OWASP Top 10 (OWASP, 2021). The text emphasizes the necessity of implementing proper encryption protocols throughout the software development lifecycle (SDLC), stressing the importance of preventing cryptographic vulnerabilities that could jeopardize sensitive information and affect regulatory compliance, such as GDPR and PCI-DSS (Allen, 2023). The discussion of encryption algorithms, particularly the vulnerability of MD5 to brute-force attacks, highlights practical security considerations in choosing robust algorithms like SHA256 (Stec, 2024).

The flowchart's structured approach, which reflects each SDLC stage and incorporates decision points for encryption and protocol selection, is commendable. This method aids developers in visualizing security as an ongoing process and understanding when and where to apply critical security measures (OWASP, 2021).

To improve the flowchart, it could benefit from more detailed annotations or visual indicators to distinguish between required steps (such as compliance checks) and recommended best practices. Additionally, incorporating an emphasis on automated testing for cryptographic strength and integrating these tests into the CI/CD pipeline could enhance its application. This addition would encourage a proactive security approach, extending beyond the design phase to encompass testing and maintenance stages (Allen, 2023).

In conclusion, your post establishes a robust framework for addressing cryptographic failures and advocates for a security-centric approach throughout the development lifecycle.

References

Allen, C. (2023) Encryption For GDPR Compliance. Cryptomathic. Available from: https://www.cryptomathic.com/blog/encryption-for-gdpr-compliance [Accessed 30 October 2024].

OWASP (2021) OWASP Top 10. OWASP. Available from: https://owasp.org/www-project-top-ten/ [Accessed 25 October 2024].

Stec, A. (2024) MD5 vs. SHA Algorithms. Baeldung. Available from: https://www.baeldung.com/cs/md5-vs-sha-algorithms [Accessed 30 October 2024].

Permalink **Show parent** **Reply**

Re: Initial Post

by George Koridze - Sunday, 3 November 2024, 7:57 PM

Your description of cryptographic failures is insightful and the flowchart effectively highlights how insufficient planning and a lack of proper encryption protocols can lead to security risks, especially in the context of GDPR compliance (Allen, 2023).

For further strengthening the prevention of cryptographic failures, data assessment action can be added to the flowchart for assessing each attribute during the planning stage to identify specific personal information that require encryption and the encryption type, per GDPR, to ensure data compliance.

Your point on using secure internet protocols (like HTTPS) during the transmission phase is spot on. Regarding your note on encryption algorithm selection, you're absolutely correct in emphasising SHA-256 over MD5 due to MD5's vulnerabilities to collision attacks (Stec, 2024), but I would also update this in the Flowchart.

Your flowchart illustrates at which stage the encryption-related risks may arise and where the secure data transmission protocols should be implemented within the SDLC process, making it easier to visualise and mitigate cryptographic vulnerabilities during planning and design phases.

References

Allen, C. (2023) Encryption For GDPR Compliance. *Cryptomathic*. Available from: **https://www.cryptomathic.com/blog/encryption-for-gdpr-compliance** [Accessed 3 November 2024]

Stec, A. (2024) MD5 vs. SHA Algorithms. *Baeldung*. Available from: **https://www.baeldung.com/cs/md5-vs-sha-algorithms** [Accessed 3 November 2024]

Permalink **Show parent** **Reply**

Peer Response

by Oi Lam Siu - Monday, 4 November 2024, 7:54 AM

Hi Anda,

Thank you for your insightful post on cryptographic failures, which you highlighted as the number two weakness in the OWASP Top 10 (OWASP, 2021). Your focus on how insufficient planning and improper encryption protocols can lead to security risks, particularly regarding GDPR compliance, is highly relevant.

I like how you emphasized the importance of identifying data safety requirements during the planning phase and the necessity of choosing secure protocols like HTTPS for data transmission. Your hands-on tips on decisions about encryption algorithms, highlighting the vulnerabilities of MD5 and the strengths of SHA-256 (Stec, 2024), provide valuable practical guidance.

In terms of improvement, as other peers mentioned, adding visual indicators to required steps and including a data assessment step during the planning stage could help identify specific personal information that requires encryption, ensuring full compliance with GDPR (Allen, 2023). Additionally, incorporating key management practices into your flowchart would enhance it further. Emphasizing the importance of secure generation, storage, and rotation of cryptographic keys is crucial, as poor key management can lead to vulnerabilities even when strong algorithms are used. Including this aspect can provide a more comprehensive view of necessary measures to prevent cryptographic failures (Barker, 2020).

Overall, your flowchart provides a solid framework for understanding where cryptographic failures can occur and how to mitigate them. By making these adjustments, it could become an even more effective tool for developers to visualize and implement security measures.

Looking forward to further discussions on this important topic.

Best regards,
Helen

Reference:

Allen, C. (2023) Encryption For GDPR Compliance. Cryptomathic. Available from: https://www.cryptomathic.com/blog/encryption-for-gdpr-compliance [Accessed 3 November 2024]

Barker, E. (2020). Recommendation for Key Management: Part 1 – General. NIST Special Publication 800-57 Part 1 Revision 5. Gaithersburg, MD: National Institute of Standards and Technology. DOI: https://doi.org/10.6028/NIST.SP.800-57pt1r5

OWASP Top 10. (2021) A07:2021 – Identification and Authentication Failures. Available from: https://owasp.org/Top10/A07_2021-Identification_and_Authentication_Failures/ [Accessed 26 October 2024]

Stec, A. (2024) MD5 vs. SHA Algorithms. Baeldung. Available from: https://www.baeldung.com/cs/md5-vs-sha-algorithms [Accessed 3 November 2024]

Maximum rating: - **Permalink** **Show parent** **Edit** **Delete** **Reply**

◄ Initial Post