

Interview Guide

Thank you for your time. We are researchers from the Ruhr University Bochum investigating the engineering process of security features in software projects. In this interview, I'd like to ask you about the process of engineering features for the software projects of your company. Specifically, we are going to focus on security features. But first, let's start our interview with some general questions about your experience and your company:

1. What is your professional background?

- (a) What is your technical background?
- (b) How much experience in years do you have in your profession?
- (c) How long have you been working in this company?

2. What kind of software do you develop?

- (a) How important is security in your projects?
- (b) Who is responsible for implementing security features?
- (c) Do you feel responsible for implementing security in the software you develop?
- (d) What frameworks or libraries do you use for your projects?
 - A. Which do you use to implement security mechanisms?

3. How are you involved in the software projects you take part in?

- (a) What are your tasks and duties?
- (b) To what extent do you consider security in your software projects?

Now that we have a rough picture of the software you develop, let me ask you more about the software engineering process:

[Explain what a security feature is: A feature implementing a specific kind of security mechanism to mitigate some kind of attack or protect some kind of asset such as personal data]

Can you name some examples of security features you develop in your projects?

1. General characteristics of security features

- (a) What are your overall security goals? (e.g., Integrity, Confidentiality, Availability)?
 - A. Why do you consider exactly these properties?
 - B. Are all properties equivalent important?
- (b) Properties of security features:
 - A. How large are security features in your system compared to functional features?
 - B. At what level of granularity are security features considered?
 - C. How are security features spread over the codebase?
 - D. How much does/is the security feature code interact/intermixed with other code? (Tangling)
 - E. How often is code reused for different security features?

2. Engineering and security practices

- (a) How does your company choose what security features to engineer?
 - A. How is it decided what security features to engineer?
 - B. On which abstraction level are security features communicated?
 - C. Who plans them?
 - D. Who is responsible for their development?
 - E. How do you prioritize security features?
 - F. Do you perform some kind of threat modelling technique?
- (b) How are security features designed?

- A. How are you involved?
- B. How are security features modeled?
- C. Which security features are challenging to plan?
- D. Are all security features equally important?
- E. Which design principles are followed?
- (c) How are security features implemented?
 - A. Which features are implemented by using a library/framework?
 - i. What role do libraries play in implementing security features?
 - ii. Which libraries are used in your software projects by developers?
 - iii. How do you use these libraries?
 - B. Are there any security features that need to be implemented from scratch?
 - i. What must be done to do so?
 - ii. Why do you implement them from scratch?
- (d) How do you test / verify the correctness of your security features?
- (e) How do you maintain your security features?

3. Challenges of engineering security features of engineering security features

- (a) What are the challenges of engineering security features?
- (b) Are all security features equally hard to engineer?
 - A. At which stage are they challenging to engineer (implementation or design)?
 - B. Why are they hard to engineer?
 - C. @devs Are there security features that look easy to implement at first, but in reality are hard to realize securely?
 - D. @sec exp What security features are underestimated concerning their secure implementation by developers?
 - E. In which security features do you detect the most bugs?
- (c) How do you handle these difficulties?
 - A. How effective is this approach?
 - B. How could it be made easier?
- (d) Which parts of the engineering process of security features could be facilitated?
 - A. What is missing for that?
 - i. What kind of tool support is missing?
 - ii. What libraries/frameworks are missing?
 - iii. What processes are missing?
 - iv. What kind of training is missing?

Is there something else you'd like to share or ask that we haven't talked about in this interview?

Again, thank you for your time and the interview. Your answers were very helpful and will aid our research tremendously. Once we complete the study, we will get back to you to share our findings.