doi:10.20396/revpibic262018450

Avaliação de ferramentas de análise de vulnerabilidades para criptografia

Ricardo Dahab, Flávia Bertoletti Silvério*.

Resumo

Há pelo menos vinte anos, estudos têm revelado que vulnerabilidades em softwares criptográficos são causadas principalmente por defeitos de implementação e pela má gestão de parâmetros criptográficos. Assim, parece ser mais fácil e prático para os atacantes cibernéticos procurarem por falhas não apenas nas implementações em software de algoritmos criptográficos, mas também, e às vezes principalmente, nas camadas de software que encapsulam, circundam ou utilizam as implementações criptográficas.

Ferramentas de análise de vulnerabilidades são incompletas, defeituosas e sem interseção entre suas regras de varredura, de modo que somente um conjunto bem escolhido de ferramentas é capaz de oferecer redundância e diversidade, promovendo a tolerância a falhas no desenvolvimento de software criptográfico. Além disso, ferramentas de análise de vulnerabilidades parecem não ser efetivas na resolução de problemas de segurança associados ao mau uso de criptografia. Existe uma lacuna entre o que os especialistas consideram como práticas ruins de programação de sistemas criptográficos e o que as ferramentas disponíveis atualmente são de fato capazes de detectar.

O objetivo deste projeto é realizar um estudo sobre as práticas ruins de criptografia detectadas por ferramentas de análise de vulnerabilidades e como programadores não especialistas são levados a utilizar criptografia de modo incorreto apesar de apoio ferramental.

Palavras-chave:

Criptografia, Programação segura, Secure Coding.