Recomendação de Segurança 001/2014 - CGTI/VPGDI

Em 1º de agosto de 2014

Para: Gestores de TI das unidades da Fiocruz

Assunto: Armazenamento de senhas

Visando a redução dos riscos no armazenamento de senhas em bancos de dados institucionais, recomenda-se a adoção de boas práticas no armazenamento de senhas de acesso, a fim de garantir a manutenção de sua confidencialidade e integridade, bem como a autenticidade das informações.

Observa-se que, por vezes, as senhas dos usuários são armazenadas em "texto claro" no banco de dados, permitindo que aqueles que tenham acesso ao banco de dados por conseguinte tenham acesso as senhas. Uma forma frequentemente adotada para mitigar tal problema é criptografar simetricamente a senha no banco de dados. No entanto, caso a chave criptográfica seja comprometida as senhas armazenadas (criptografadas) poderão ser reveladas.

Com o uso da função *hash* é possível aumentar substancialmente a confidencialidade das senhas, pois através do *hash* não é preciso armazenar a senha dos usuários no banco, mas sim o resultado de sua função sobre a senha. Por exemplo: a função *hash* da palavra "password" utilizando o algoritmo SHA1 apresenta como resultado a expressão `5BAA61E4C9B93F3F0682250B6CF8331B7EE68FD8`. Com o *hash* da senha armazenado no banco de dados, quando um usuário se logar na aplicação, é possível que esta gere o *hash* da senha inserida pelo usuário e compare com a informação armazenada no banco de dados (*hash* da senha armazenada), autenticando o usuário caso os valores coincidam.

Uma propriedade do *hash* é ser unidirecional, ou seja, não é possível obter o dado original a partir do resumo gerado. Sendo assim, dado um valor de *hash*, não é possível descobrir o texto original. O algoritmo de *hash* ideal é aquele que apresenta o menor índice de colisões. Uma colisão ocorre quando duas palavras diferentes geram um mesmo *hash*.

Apesar do armazenamento do *hash* ser um grande avanço, ainda não é a melhor solução, pois a partir de um ataque conhecido como *Rainbow Table* é possível usar um dicionário com milhares ou até mesmo milhões de palavras com seus respectivos *hash*. Assim, é possível comparar o *hash* do dicionário com o *hash* armazenado e descobrir a senha.

Desta forma, a recomendação para o armazenamento de senhas é combinar o *hash* da senha com o que chamamos de "*salt*". O *salt* é uma *string* complexa e aleatória que será concatenada à senha antes de criptografá-la. Dessa forma, cada senha terá o seu próprio *salt* e para descobrir a senha o atacante terá que gerar uma *Rainbow Table* para cada *salt*, aumentando a complexidade do processo a um nível que, se combinado a outras práticas (troca periódica das senhas, uso de senhas fortes, etc.), torna o esforço para quebra de senha inviável para o atacante.

Atenciosamente,

Coordenação de Gestão de Tecnologia da Informação
Segurança da Informação e Comunicações