Lista 07

Vinícius de Oliveira Peixoto Rodrigues (245294)

Setembro de 2022

Questão 1

As formas 1 e 2 são vulneráveis a spoofing por meio de um oracle attack:

- Ana A tenta iniciar uma conexão com Beto B; Caio intercepta a comunicação
- $A \to C(B) : N_a$ (Caio se passando por Beto)
  - Caio abre paralelamente uma transação de autenticação, se passando por Ana:
  - $C(A) \to B : N_a$
  - $B \to C(A) : E_k(N_a)$ (Caio obtém a resposta $E_k(N_a)$)
- $C(B) \to A : E_k(N_a)$ (Caio efetivamente se passa por Beto)

A mesma ideia pode ser usada na forma 2.

Essa vulnerabilidade vem do fato de que tanto na forma 1 quanto na forma 2, Beto está disposto a encriptar/decriptar o nonce de Ana "sem questionamentos". Isso pode ser resolvido na forma 3 por meio da função $f(N_a)$, que deve "acoplar"mais fortemente a mensagem ao destinatário (por exemplo, encriptando o nonce com a chave pública de Ana).

Questão 2

Mesmo que a chave não tenha sido transmitida, esse esquema é vulnerável caso alguém consiga fazer sniffing das mensagens de handshake:

- Ana tem chave de sessão K, número aleatório A
- Ana gera $T = K \oplus A$ e envia para Beto
- Caio escuta e guarda T
- Beto envia de volta o valor A obtido a partir de K
- Caio escuta, guarda A e calcula $T \oplus A = K$, obtendo a chave secreta

Questão 4

Para propósitos de correção de erro, faz pouco sentido implementar um ECC interno, visto que é mais provável que haja erros na transmissão do pacote já encriptado (e se houver, o erro vai se propagar e invalidar o ECC). Faz mais sentido implementar ECC externamente, concatenando o ECC e a mensagem cifrada.

Questão 5