**TAREFA 4 (Individual) – SEGURANÇA DE ACESSO REMOTO**

ESTUDO-DE-CASO: SEGURANÇA DE TERMINAIS E CAIXAS AUTOMÁTICOS

**OBJETIVOS:**

1. As primeiras abstrações de protocolos criptográficos.
2. Mostrar alguns aspectos sobre autenticação de usuário de um sistema.
3. Mostrar onde criptografia simétrica e assimétrica podem ser usadas.
4. Mostrar uma técnica de autenticação de dados invariantes no tempo.
5. Mostrar a possibilidade de algumas formas de ataque sobre os protocolos de autenticação
 ilustrados.
 **AVALIAÇÃO:** Numa nota de 0-100, as questões valem:
(8) 10, (13) 20, (15) 20, (17) 10, (19) 10, e as demais valem 2.

**Considere os arquivos CripSimCE0001, CripSimCE0002 e CripSimCE0003

Questões a Responder:**

1. **Leia o texto que descreve o protocolo abaixo no arquivo CripSimCE0001. Que forma de criptografia você vislumbra, estando sendo usada no caso deste protocolo de autenticação ?**

 **Figura 1- Um Protocolo de Autenticação do Usuário
 CA(r) significa r sendo cifrado com a chave CA**

1. **Que tipo de chave parece ser a chave CA ou que função tem a chave CA neste protocolo ? Existe autenticação mútua neste protocolo ?**
2. **Por que o número aleatório r deve ser gerado pelo terminal ?**
3. **No protocolo da seção 3 (figura 1) se r for eliminado das mensagens, um atacante pode gravar a sessão de um usuário A, e mais tarde numa segunda sessão, fazer-se passar pelo sistema perante A. Que nome se dá a esse ataque ? Pesquise por ataque “man-in-the-middle” e verifique se esta forma de ataque tem cabimento neste caso.**
4. **Por que o número aleatório r´ deve ser gerado pelo sistema ?**
5. **No protocolo da seção 3 (figura 1), se r´ for eliminado das mensagens, um atacante pode gravar a sessão de um usuário A, e mais tarde numa segunda sessão, fazer-se passar por A perante o sistema. Que nome se dá a esse ataque ? Pesquise o que é um ataque de repetição e verifique se é possível ocorrer esta forma de ataque.**
6. **Que forma de ameaça (Fraude, Desfalque ou Falsificação) é mais suscetível de ocorrer, no caso do número aleatório r´ ser eliminado. Ver as definições dessas ameaças nos slides mostrados em aula.**
7. **Descreva o protocolo da figura 1 ao caso da criptografia de chave pública, ao invés de criptografia de chave simétrica.**
8. **Como o arquivo original de senhas pode ser protegido ?**
9. **Que tipo de função matemática tem sentido para garantir segurança neste contexto, ou seja, por que a proteção funciona para proteger o arquivo original de senhas ?**
10. **Descreva como um atacante pode alterar o arquivo de senhas cifradas ?**
11. **Que técnica é conhecida para evitar este tipo de ataque, em que o sistema permite verificar se uma informação foi ou não alterada ?**
12. **Descreva a técnica que permite verificar que uma informação foi alterada num sistema de criptografia simétrica.**
13. **Como um atacante pode ainda fazer com que o esquema da técnica de autenticação de dados invariantes com o tempo não seja mais seguro ?**
14. **Descreva um mecanismo de autenticação de dados invariantes com o tempo, baseado num sistema de criptografia de chave pública. Nesta caso, é ainda necessário um dispositivo criptográfico inviolável que gera uma chave mestra secreta CT no terminal ?**
15. **Seja outro protocolo de autenticação Terminal-Sistema, como mostra a figura 3, no que segue. Leia o texto do protocolo no arquivo CripSimCE0001.**

****

 **Figura 3 – Outro protocolo de autenticação do usuário**

**Que vantagem o protocolo da figura 3 apresenta em relação ao protocolo da figura 1 ?**

1. **Descrever este protocolo (figura 3) para o caso da criptografia de chave pública.**
2. **Descrever o ataque que pode acontecer, se no protocolo da figura 3, o valor de r for eliminado.**
3. **Mais ainda, r não deve ser fornecido pelo usuário, mas gerado pelo terminal. Descreva o ataque que pode ocorrer, supondo o contrário, isto é, que o usuário é que fornece o número r.**
4. **Como o ataque da questão 20, pode ser impedido ? Considere a informação n que um usuário deve entrar no terminal, antes deste calcular o número aleatório r.**

**Analogamente, ao que acontece no protocolo da figura 1, onde chaves precisam ser protegidas no sistema central, a chave CA necessitava de proteção. No protocolo da figura 3, CT necessita ser protegida. Proteção de chaves é outro assunto importante que pode ser abordado, mas que não está sendo tratado aqui.**