Redes de Computadores II: Segunda Lista de Exercícios

Prof. Diego Passos, Universidade Federal Fluminense 2/2015

1. Defina o conceito de **confidencialidade** no contexto de segurança em redes.
2. Defina o conceito de **autenticidade** no contexto de segurança em redes.
3. Defina o conceito de **integridade** no contexto de segurança em redes.
4. Defina o conceito de **disponibilidade** no contexto de segurança em redes.
5. Defina o que é um ataque de negação de serviço.
6. Discuta a afirmação: ataques de negação de serviço sempre são baseados na sobrecarga do serviço por parte do atacante.
7. O único objetivo da criptografia é a confidencialidade? Em caso negativo, cite outras aplicações da criptografia no contexto da segurança em redes.
8. O que é uma chave criptográfica?
9. Algoritmos de criptografia são normalmente classificados em algoritmos de chave simétrica e algoritmos de chave pública. Quais são as diferenças, vantagens e desvantagens destas duas classes?
10. Uma **cifra de substituição** é um algoritmo criptográfico simples, baseado em chave simétrica. A chave, neste caso, é uma **permutação do alfabeto** utilizado para criar as mensagens. Para cifrar uma mensagem em texto plano, cada símbolo (letra) da mensagem é substituído pelo símbolo na mesma posição do alfabeto permutado. Suponha que você tenha que implementar este método criptográfico para garantir a confidencialidade de certas comunicações. Como sua implementação geraria as chaves? Há alguma restrição na escolha de uma chave? Existem chaves "ruins"?
11. Ainda sobre as cifras de substituição, suponha que um atacante (Trudy) fosse capaz de executar um **ataque de texto plano escolhido** sobre a cifra. Isto é, digamos que Alice e Bob escolherem uma chave para a cifra de substituição e Trudy, de alguma forma, é capaz de forçar Alice a cifrar mensagens quaisquer e obter o texto cifrado correspondente. A cifra de substituição é vulnerável a este tipo de ataque? Explique como Trudy poderia usar este ataque para quebrar a criptografia da comunicação entre Alice e Bob.
12. Suponha que uma determinada aplicação implementa e utiliza o algoritmo RSA com uma chave cujo componente n (o módulo utilizado para cifrar/decifrar mensagens) é um número de 1024 bits. Nestas condições, responda:

a) Qual é, em número de bits, o tamanho máximo de uma mensagem que pode ser cifrada (isto é, sem ser quebrada)?

b) Qual é, em número de bits, o tamanho mínimo de uma mensagem que pode ser cifrada (isto é, sem ser quebrada)?

c) Qual é, em número de bits, o tamanho máximo de uma mensagem cifrada gerada por esta aplicação (assumindo que o texto plano correspondente não tenha sido quebrado)?

13. Suponha que você deseje criar um par de chaves pública e privada para utilizar com o algoritmo RSA para ilustrar a alguém o funcionamento do algoritmo. Para que as operações possam ser feitas de forma mais fácil, você decide criar chaves pequenas e escolhe $p = 3$ e $q = 5$, resultando em $n = 15$ e $z = 8$. Ainda seguindo os passos para geração de uma chave, você arbitra que $e = 5$ e verifica que $d = 5$ atende à condição de que $de \equiv 1 \ (mod \ z)$. Em resumo, você gerou as chaves pública $(n = 15, e = 5)$ e privada $(n = 15, d = 5)$ (em outras palavras, ambas as chaves são iguais). Como você seguiu todas as instruções para a geração de chaves, as propriedades do RSA ainda se aplicam (*i.e.*, o algoritmo ainda funciona). Mas você vê algum problema no uso desta chave? Se a mesmo ocorresse na geração de uma chave longa (*e.g.*, de 4096 bits), você se sentiria seguro utilizando esta chave? Discuta.

14. Por que em certas aplicações algoritmos de criptografia de chave pública são utilizados apenas para o estabelecimento de chaves simétricas de sessão?

15. Explique o que é um ataque de repetição.

16. O que é um *nonce*? Explique como *nonces* podem ser utilizados em um processo de autenticação de um servidor com um *browser*, assumindo que o *browser* conheça previamente a chave pública do servidor.

17. O que é um ataque do tipo *man-in-the-middle*?

18. Explique como funciona uma assinatura digital e como ela pode ser usada para garantir a integridade de uma mensagem recebida.

19. Considere a possibilidade de utilizarmos o *Checksum* da Internet como um método de resumo criptográfico em uma assinatura digital. Lembre-se que o *Checksum* da Internet é basicamente uma soma feita em blocos de dois bytes ao longo de toda a mensagem. Assuma que Alice envia para Bob a seguinte sequência de bytes assinados digitalmente (utilizando o Checksum da Internet como resumo criptográfico): $65_{(16)} \ 54_{(16)} \ F5_{(16)} \ AC_{(16)}$. Considere ainda que Trudy queira fazer uma modificação qualquer nesta mensagem de forma que a assinatura digital ainda bata. Mostre uma possível versão alterada desta mensagem que atenda a estes requisitos.

20. O que é um MAC (*Message Authentication Code*)? Como este método funciona?

21. O que é certificado digital. E uma autoridade certificadora? Como ambos podem ser usados para garantir a autenticidade de uma chave pública?

22. O que são certificados raiz?

23. Suponha que sua máquina tenha sido invadida e os certificados raiz armazenados no seu *browser* tenham sido alterados. Quais as possíveis consequências disto?

24. Suponha agora que o computador que armazena a chave privada de uma entidade certificadora tenha sido invadido e a chave tenha sido comprometida. Quais as consequências disso?

25. Por que razão certificados possuem as datas de emissão e expiração? Cite alguns motivos.

26. Do que consiste a revocação de um certificado? Explique como este processo é feito através das CRLs e cite alguns motivos para que um certificado seja revogado.

27. Qual é o objetivo do algoritmo de Diffie-Hellman? O algoritmo sempre funciona ou é susceptível a algum tipo de ataque?

28. No contexto de segurança em redes, o que é *forward secrecy*? Dê um exemplo.

29. Explique como as aplicações de e-mails seguro são capazes de prover, simultaneamente, confidencialidade, integridade e autenticidade da mensagem.

30. O que é SSL? Quais são as principais vantagens de uma solução de segurança como o SSL?

31. Quantas chaves e com quais funções fazem parte de uma conexão SSL?

32. Qual método de verificação de integridade é utilizado no SSL?

33. No SSL, o fluxo de dados de uma conexão é quebrado em registros. Cada registro possui sua própria verificação de integridade. Explique a razão para esta abordagem (ao invés de usar apenas uma grande verificação de integridade para toda a conexão.

34. Na verificação de integridade de mensagens, o SSL computa o *hash* da mensagem concatenada com um número de sequência. No entanto, não existe um campo de número de sequência no SSL. Explique qual é a utilidade de se incluir este número de sequência no compto do *hash* e como o receptor é capaz de verificar a integridade do registro se o número de sequência não é explicitamente informado no registro.

35. O SSL utiliza *nonces*? Por que?

36. Por que o *handshake* do SSL precisa de verificação de integridade?

37. Assuma que um atacante seja capaz de forjar um pacote sinalizando o fechamento de uma conexão TCP que transporta uma comunicação SSL. Como o SSL se protege deste tipo de ataque?

38. O que são e quais são os propósitos das VPNs?

39. O IPSec é um protocolo orientado a conexão. Por que?

40. Para que serve o campo SPI em um cabeçalho IPSec?

41. No modo túnel do IPSec com ESP, todo o datagrama original a ser enviado é criptografado e autenticado (através de um MAC). Mas os campos do cabeçalho IPSec são apenas autenticados. Por que não há criptografia nestes campos?

42. No WEP, qual é a utilidade do campo IV?

43. Há vários programas disponíveis na Internet que implementam ataques ao WEP. A maioria deles procura coletar um grande número de quadros legítimos antes de analisá-los tentando obter a chave pré-compartilhada. Qual é o objetivo desta captura prévia de pacotes? O que o atacante busca com isso? Como isso auxilia no processo de quebra da chave?

44. Explique de forma geral como funciona o modo *Enterprise* do WPA/WPA2.

45. Discuta a afirmação: embora o WPA Personal seja mais seguro que o WEP, a utilização de chaves pré-compartilhadas é inerentemente insegura.

46. O que é um *firewall*? Quais as diferenças entre um *firewall stateful* e *stateless*?

47. O que é um *gateway de aplicação*? Como isso se diferencia de um *firewall* "comum"?

48. Suponha que você é o administrador de uma rede. Em um dado momento, você percebe que sua rede está recebendo um tráfego externo anômalo: um grande volume de segmentos TCP são recebidos por determinados servidores, sem que conexões correspondentes tenham sido previamente abertas. Você decide, então, resolver este problema através da inserção de uma ou mais regras de *firewall* no roteador de borda da rede. Nestas condições, responda:

    a) Você precisa de um *firewall stateful* ou *stateless* para esta funcionalidade? Justifique.

    b) Explique como seria a regra utilizada para realizar este bloqueio (*i.e.*, que tipo de informações o *firewall* deverá verificar para cada pacote).

49. Nos sistemas Linux, *firewalls* são normalmente implantados através de um *software* chamado *iptables*. O *iptables* também é comumente utilizado para implementar NAT (além do controle de admissão dos pacotes, o *iptables* permite que certas modificações sejam realizas em cada pacote). Com base nestas informações apenas, você diria que o *iptables* consiste em um *firewall stateful* ou *stateless*?

50. O que são os IDSs? Que tipo de ataque eles tentam coibir?

51. Conforme visto ao longo das aulas, técnicas de segurança podem ser implementadas em diversas camadas da pilha de protocolos TCP/IP. Discuta as vantagens e desvantagens

da implementação de medidas de segurança nas camadas de Transporte (*e.g.*, SSL), rede (*e.g.*, IPSec), e enlace (*e.g.*, WPA no IEEE 802.11). Procure mostrar as garantias de segurança que a implementação de cada camada oferece em relação às demais.

52. Suponha que Alice deseja enviar uma mensagem m para Bob de forma segura. Assuma que, de alguma forma, Alice conhece a chave pública correta de Bob e Bob conhece a chave pública correta de Alice. Para cada um dos casos a seguir, explique como Alice e Bob podem conseguir estabelecer esta comunicação segura, destacando as chaves utilizadas (*e.g.*, chave pública Bob, chave simétrica compartilhada) e em que momentos elas são utilizadas por cada parte na comunicação.

    a) Bob e Alice desejam **apenas** confidencialidade.

    b) Bob deseja **apenas** ser capaz de autenticar a mensagem como sendo originada por Alice.

    c) Bob deseja **apenas** ser capaz de autenticar a mensagem como sendo originada por Alice e verificar a integridade da mensagem.

    d) Bob e Alice desejam garantir **simultaneamente** confidencialidade, autenticidade (*i.e.*, Bob deve ser capaz de verificar que a mensagem foi originada por Alice), e integridade.

53. Considere novamente uma comunicação entre Alice e Bob. Novamente, assuma que, de alguma forma, Alice conhece a chave pública correta de Bob e Bob conhece a chave pública correta de Alice. Após criar a mensagem m que deseja enviar para Bob, Alice a cifra com sua chave privada, obtendo $K_A^-(m)$. Este resultado é, então, cifrado com a chave pública de Bob, resultando em $K_B^+(K_A^-(m))$. Finalmente, Alice calcula um *hash* criptográfico $H(K_B^+(K_A^-(m)))$ sobre o resultado anterior. Após todas estas computações, Alice envia para Bob ambos $K_B^+(K_A^-(m))$ e $H(K_B^+(K_A^-(m)))$. Ao receber este par de informações, Bob calcula o mesmo *hash* criptográfico de $K_B^+(K_A^-(m))$ e compara o resultado ao *hash* recebido. Adicionalmente, Bob decifra $K_B^+(K_A^-(m))$ primeiramente com sua chave privada e, em seguida, com a chave pública de Alice. Nestas condições, responda justificando:

    a) Este processo garante confidencialidade?

    b) Este processo permite a verificação da integridade da mensagem por parte de Bob?

    c) Este processo permite que Alice autentique o receptor como sendo Bob?

    d) Este processo permite que Bob autentique Alice como sendo a origem da mensagem?