Estudo dirigido sobre o capítulo 8 (parte 2) – segurança de redes

INSTITUTO FEDERAL
RIO GRANDE DO SUL

1. Qual é a forma definitiva para se obter confidencialidade na troca de e-mails?

- Alice:

1. escolhe uma chave simétrica, K_s, aleatoriamente

2. criptografa sua mensagem m com a chave simétrica K_s

3. criptografa a chave simétrica com a chave pública de Bob

4. concatena a mensagem criptografada e a chave simétrica criptografada de modo que formem um pacote; e

5. envia o pacote ao endereço de e-mail de Bob

1. Qual é a forma definitiva para se obter confidencialidade na troca de e-mails?

- Bob:

1. usará sua chave privada para obter a chave simétrica K_s

2. utilizará a chave simétrica K_s para decodificar a mensagem m

2. Como se fornece autenticação do remetente e também integridade da mensagem no sistema de e-mail seguro?

- Alice:

1. aplica uma função de *hash* H (por exemplo, MD5) à sua mensagem m, para obter um resumo de mensagem

2. assina o resultado da função de *hash* com sua chave privada para criar uma assinatura digital

3. concatena a mensagem original (não criptografada) com a assinatura para criar um pacote; e

4. envia o pacote ao endereço de e-mail de Bob

2. Como se fornece autenticação do remetente e também integridade da mensagem no sistema de e-mail seguro?

- Bob:

1. aplica a chave pública de Alice ao resumo de mensagem assinado

2. compara o resultado dessa operação com o próprio *hash* H da mensagem

3. Como se fornece confidencialidade, autenticação do remetente e também integridade da mensagem no sistema de e-mail seguro?

- Isso pode ser feito pela combinação dos procedimentos descritos nas questões 1 e 2

4. O que é o PGP e quais algoritmos ele utiliza?

- Projetado originalmente por Phil Zimmermann em 1991, o PGP (*Pretty Good Privacy* – privacidade razoável) é um esquema de criptografia para e-mail que se tornou um padrão de fato
- O projeto do PGP é, em essência, idêntico ao projeto descrito nas questões anteriores
- Dependendo da versão, o software do PGP usa MD5 ou SHA para processar o resumo de mensagem; CAST, DES triplo ou IDEA para criptografar chaves simétricas e RSA para criptografar chaves públicas

5. Descreva o funcionamento do PGP (após sua instalação)?

- Quando o PGP é instalado, ele cria um par de chaves para o usuário
- A chave pública pode então ser colocada no site do usuário ou em um servidor de chaves públicas
- A chave privada é protegida pelo uso de uma senha, que tem de ser informada todas as vezes que o usuário acessar a chave privada
- O PGP oferece ao usuário a opção de assinar digitalmente a mensagem, criptografar a mensagem ou, ainda, ambas as opções
- OpenPGP (*www.openpgp.org*)

6. O que é o SSL? Como identificar o seu uso?

- É uma versão aprimorada do TCP denominada Camada Segura de Sockets (*Secure Sockets Layer* – SSL)
  - Uma versão levemente modificada da versão 3 do SSL, denominada Segurança na Camada de Transporte (*Transport Layer Security* – TLS) foi padronizada pelo IETF
- Você pode identificar que o SSL está sendo usado por seu browser quando a URL se iniciar com https: em vez de http:

7. Quais são os possíveis problemas de uma compra com cartão pela Internet?

- Se nenhum sigilo (encriptação) for utilizado, um invasor poderia interceptar o pedido de Bob e receber suas informações sobre o cartão
  - O invasor poderia, então, fazer compras à custa de Bob
- Se nenhuma integridade de dados for utilizada, um invasor poderia modificar o pedido de Bob, fazendo-o comprar dez vezes mais frascos de perfumes que o desejado
- Finalmente, se nenhuma autenticação do servidor for utilizada, um servidor poderia exibir o logo de Alice, quando na verdade o site é mantido por Trudy
  - Após receber o pedido de Bob, Trudy poderia ficar com o dinheiro dele e sumir
  - Ou Trudy poderia realizar um roubo de identidade obtendo o nome, endereço e o número do cartão de Bob

8. É apenas o HTTP que pode fazer uso de SSL?

- Como o SSL protege o TCP, ele pode ser empregado por qualquer aplicação que execute o TCP
- O SSL provê uma API com *sockets*, semelhante ao API do TCP
- Quando uma aplicação quer empregar o SSL, ela inclui classes/bibliotecas SSL
- Da perspectiva do desenvolvedor, o SSL é um protocolo de transporte que provê serviços do TCP aprimorados com serviços de segurança

9. Descreva as etapas da verdadeira apresentação SSL.

- 1. o cliente envia uma lista de algoritmos criptográficos que ele suporta, junto com um nonce do cliente
- 2. a partir da lista, o servidor escolhe um algoritmo simétrico, um algoritmo de chave pública e um algoritmo MAC
  - Ele devolve ao cliente suas escolhas, bem como um certificado e um nonce do servidor
- 3. O cliente verifica o certificado, extrai a chave pública do servidor, gera um Segredo Pré-Mestre (PMS), cifra o PMS com a chave pública do servidor e envia o PMS cifrado ao servidor

9. Descreva as etapas da verdadeira apresentação SSL.

- 4. Utilizando uma função de derivação de chave, o cliente e o servidor computam independentemente o Segredo Mestre (MS) do PMS e dos *nonces*
  - O PMS é então dividido para gerar as duas chaves de criptografia e duas chaves MAC
  - De agora em diante, todas as mensagens enviadas entre o cliente e o servidor são cifradas e autenticadas (com o MAC)
- 5. o cliente envia um MAC de todas as mensagens de apresentação
- 6. o servidor envia um MAC de todas as mensagens de apresentação

9. Descreva as etapas da verdadeira apresentação SSL.

- https://cryptoid.com.br/banco-de-noticias/o-que-e-ssl-tls-e-por-que-e-hora-de-atualizar-para-tls-1-3/

10. Para que é usado o IPSec?

- Para a criação de redes virtuais privadas (VPNs) que são executas por meio da Internet pública
- https://tools.ietf.org/html/rfc6071

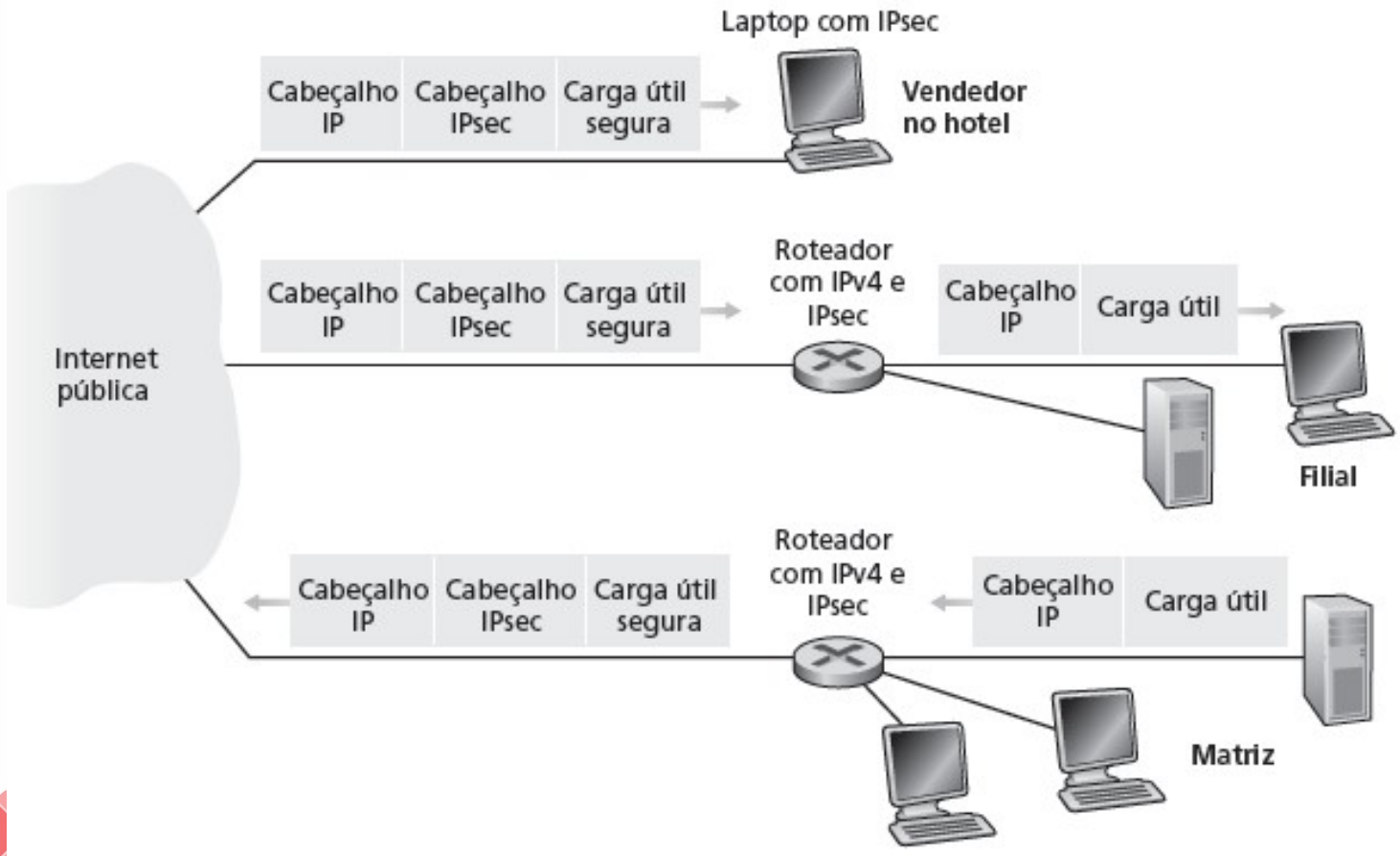
11. Por que a segurança na camada de rede é conhecida por prover “cobertura total”?

- Com o sigilo da camada de rede entre um par de entidades de rede, a entidade remetente cifra as cargas úteis de todos os datagramas que envia à entidade destinatária
- A carga útil cifrada poderia ser um segmento TCP, um segmento UDP e uma mensagem ICMP, etc
- Se esse serviço de camada de rede estivesse em funcionamento, todos os dados de uma entidade a outra – incluindo e-mail, páginas Web, mensagens de apresentação TCP e mensagens de gerenciamento (como ICMP e SNMP) – estariam ocultos de qualquer terceira parte que possa estar analisando a rede
- Por esta razão, a segurança na camada de rede é conhecida por prover “cobertura total”

12. Descreva uma VPN. Qual seria a sua alternativa?

- A instituição poderia empregar uma rede física independente – incluindo roteadores, enlaces e uma infraestrutura DNS – que é completamente distinta da Internet pública
- Essa rede disjunta, reservada a uma instituição particular, é chamada de rede privada
- Como é de se esperar, uma rede privada pode ser muito cara
- Com uma VPN, o tráfego interdepartamental é enviado por meio da Internet pública e não de uma rede fisicamente independente
- Mas, para prover sigilo, o tráfego interdepartamental é criptografado antes de entrar na Internet pública

12. Descreva uma VPN. Qual seria a sua alternativa?



13. Por que a segurança é uma preocupação especialmente importante em redes sem fio?

- Segurança é uma preocupação importante em redes sem fio, onde as ondas de rádio carregando quadros podem propagar muito além da construção contendo os hospedeiros e as estações sem fio

14. Como é realizada a autenticação no WEP (*deprecated*)?

1. Um hospedeiro sem fio requisita uma autenticação por um ponto de acesso

2. O ponto de acesso responde à requisição de autenticação com um valor de 128 bytes *nonce*

3. O hospedeiro sem fio criptografa o *nonce* usando uma chave simétrica que compartilha com o ponto de acesso

4. O ponto de acesso decriptografa o *nonce* do hospedeiro

15. O que é um firewall?

- Um *firewall* é uma combinação de hardware e software que isola a rede interna de uma organização da Internet em geral, permitindo que alguns pacotes passem e bloqueando outros
- Um *firewall* permite que um administrador de rede controle o acesso entre o mundo externo e os recursos da rede que administra gerenciando o fluxo de tráfego de e para esses recursos

16. Quais são os seus objetivos (de um *firewall*)?

- Todo o tráfego de fora para dentro, e vice-versa, passa por um *firewall*
- Somente o tráfego autorizado, como definido pela política de segurança local, poderá passar
- O próprio *firewall* é um mecanismo conectado à rede
  - Se não for projetado ou instalado adequadamente, ele pode ser comprometedor

17. Quais são as três categorias de *firewall*?

- Os *firewalls* podem ser classificados em três categorias: filtros de pacote tradicionais, filtros de estado e *gateways* de aplicação

18. Em que são baseadas as decisões de filtragem em filtros de pacote?

- Um filtro de pacote examina cada datagrama que está sozinho, determinando se o datagrama deve passar ou ficar baseado nas regras específicas do administrador
- As decisões de filtragem são normalmente baseadas em:
  - Endereço IP de origem e de destino
  - Tipo de protocolo no campo do datagrama IP: TCP, UDP, ICMP, OSPF, etc
  - Porta TCP ou UDP de origem e de destino
  - Bits de flag do TCP: SYN, ACK, etc
  - Tipo de mensagem ICMP
  - Regras diferentes para datagramas que entram e saem da rede
  - Regras diferentes para interfaces do roteador distintas

19. Qual é a base do funcionamento de um filtro de pacote com controle de estado? Dê um exemplo.

- Os filtros de estado rastreiam conexões TCP e usam esse conhecimento para tomar decisões sobre filtragem
- Um atacante que tenta enviar um pacote defeituoso para a rede da organização por meio de um datagrama com porta de origem 80 e com o flag ACK definido
- Suponha que este pacote possua um número de porta de origem 12543 e endereço IP remetente 150.23.23.155
- Quando este pacote chega ao firewall, este verifica a lista de controle de acesso e uma tabela de conexões e observa que esse pacote não faz parte de uma conexão TCP em andamento e o rejeita

20. O que é um *gateway* de aplicação? Exemplifique *gateways* de aplicação comuns.

- E se uma organização quiser fornecer o serviço Telnet a um conjunto restrito de usuários internos (em vez de endereços IP)?
- *Gateways* de aplicação fazem mais do que examinar cabeçalhos IP/TCP/UDP e tomam decisões com base em dados da aplicação
- Um *gateway* de aplicação é um servidor específico de aplicação através do qual todos os dados da aplicação (que entram e que saem) devem passar

20. O que é um *gateway* de aplicação? Exemplifique *gateways* de aplicação comuns.

- *Gateway* telnet: o filtro do roteador está configurado para bloquear todas as conexões Telnet, exceto aquelas que se originam do *gateway* de aplicação
- Essa configuração de filtro força todas as conexões Telnet de saída a passarem pelo *gateway* de aplicação
- Considere agora um usuário interno que queira executar Telnet com o mundo exterior
- Em primeiro lugar, ele tem de estabelecer uma sessão Telnet com o gateway de aplicação
- Uma aplicação que está executando no *gateway* – e que fica à escuta de sessões Telnet que entram – solicita ao usuário sua identificação e senha
- Se o usuário tiver permissão, o *gateway* torna-se um intermediário da conexão Telnet, atuando como servidor e cliente Telnet ao mesmo tempo
- Redes internas frequentemente têm vários *gateways* de aplicação, como *gateways* para Telnet, HTTP, FTP e e-mail

21. Dê um exemplo de funcionamento de um *gateway* de aplicação.

- Já apresentado na resposta da questão 20

22. O que é um IDS? E um IPS?

- Para detectar muitos tipos de ataque, é necessário executar uma inspeção profunda de pacote, isto é, olhar através dos campos de cabeçalho e dentro dos dados da aplicação que o pacote carrega
- Um *gateway* de aplicação só executa isto para uma aplicação específica
- Um dispositivo que gera alertas quando observa tráfegos potencialmente mal intencionados é chamado de sistema de detecção de instrusos (IDS – *instrusion detection system*)
- Um dispositivo que filtra o tráfego suspeito é chamado de sistema de prevenção de intrusão (IPS – *intrusion prevention system*)

23. Qual é a operação de um IDS baseado em assinatura?

- Cada assinatura é um conjunto de regras relacionadas a uma atividade de instrusos
- Uma assinatura pode ser uma lista de características sobre um único pacote (por exemplo, números de portas de origem e destino, tipo de protocolo, e uma sequência de bits em uma carga útil de um pacote)
- Um IDS baseado em assinatura analisa cada pacote que passa, comparando cada pacote analisado com as assinaturas no banco de dados
- Se um pacote (ou uma série deles) é compatível com uma assinatura no banco de dados, o IDS gera um alerta

24. Quais são as desvantagens de IDS baseado em assinatura?

- Ele é completamente cego a novos ataques que ainda não foram registrados
- E, mesmo se uma assinatura for compatível, pode não ser o resultado de um ataque, mas mesmo assim um alarme é gerado
- Finalmente, pelo fato de cada pacote ser comparado com uma ampla coleção de assinaturas, o IDS fica pressionado com processamento e falha na detecção de muitos pacotes malignos

25. Como trabalha um IDS baseado em anomalias?

- Um IDS baseado em anomalias cria um perfil de tráfego enquanto observa o tráfego em operação normal
- Ele procura então por cadeias de pacote que são estatisticamente incomuns, por exemplo, uma porcentagem irregular de pacotes ICMP ou um crescimento exponencial de *scanners* de porta e varreduras de *ping*
- Eles não recorrem a conhecimentos prévios de outros ataques
- https://www.addictivetips.com/net-admin/intrusion-detection-tools/
- https://www.addictivetips.com/net-admin/intrusion-prevention-systems/