Segurança em Redes

Aula 13 - Segurança no Serviço de Correio Eletrônico

Apresentação

Nesta aula, iremos realizar uma breve revisão sobre o conjunto de protocolos utilizados na implementação de serviços de correio eletrônico, a saber: SMTP, POP3 e IMAP, com foco em seus problemas de segurança. Em seguida, estudaremos as principais soluções criadas para esses problemas, que, basicamente, fazem uso de mecanismos de autenticação e criptografia.

Vídeo 01 - Apresentação

Objetivos

Ao final desta aula, você será capaz de:

- Relembrar os principais conceitos de funcionamento dos protocolos utilizados para o envio (SMTP) e leitura (POP3 e IMAP) de e-mails.
- Conhecer seus principais problemas de segurança.
- Conhecer as principais soluções atualmente disponíveis para esses problemas.

Conceito de Segurança em Correio Eletrônico

Na disciplina de redes de computadores, você estudou um serviço que já devia utilizar, ou pelo menos conhecer, mesmo antes de iniciar este curso: o serviço de correio eletrônico, conhecido popularmente como *serviço de e-mail*. Na aula sobre o serviço de coreio eletrônico você aprendeu, entre outras coisas, como é formado um endereço eletrônico, bem como o formato das mensagens (e-mails) trocadas entre os clientes e servidores desse serviço. Você também estudou sobre os clientes desse serviço, que podem ser instalados utilizando programas específicos, como o Outlook ou *Thunderbird,* ou serem acessados pelo browser (serviços de webmail). Também foi apresentada a sequência de passos seguidos pelos clientes e servidores de SMTP, para o envio de uma mensagem até que ela chegue ao seu destino. Por fim, você estudou que para a leitura de e-mails são utilizados os protocolos POP3 ou IMAP, sendo eles completamente independentes do SMTP.

Nesta aula, iremos discutir os principais problemas de segurança que afetam esses três protocolos, bem como algumas das soluções atualmente em uso. Dado que estamos estudando protocolos independentes, também dividiremos nossa aula em dois tópicos principais:

- **Segurança na leitura de e-mails:** necessária na comunicação entre clientes e servidores de e-mail, e no uso dos protocolos POP3S e IMAPS (que serão apresentados).

- **Segurança no envio de email:** necessária na comunicação entre clientes e servidores, bem como entre servidores de e-mail. Na nossa aula, iremos focar em diversos mecanismos e técnicas utilizadas para controlar o envio e o recebimento de mensagens indesejadas, os famosos e já bastante estudados SPAM.

Vídeo 02 - Revisão

Atividade 01

1. Por que os problemas de segurança relacionados à leitura e envio de e-mails são distintos?

Segurança na Leitura de E-mails

A segurança nos protocolos utilizados para leitura de e-mails é conseguida pela adição de novos conjuntos de funcionalidades ao POP3 e IMAP. Apesar de conceitualmente não ter sido definido nenhum novo protocolo, é comum utilizarmos os termos POP3S e IMAPS, quando nos referimos ao uso dos protocolos originais, com os novos conjuntos de funcionalidades, ligados à segurança.

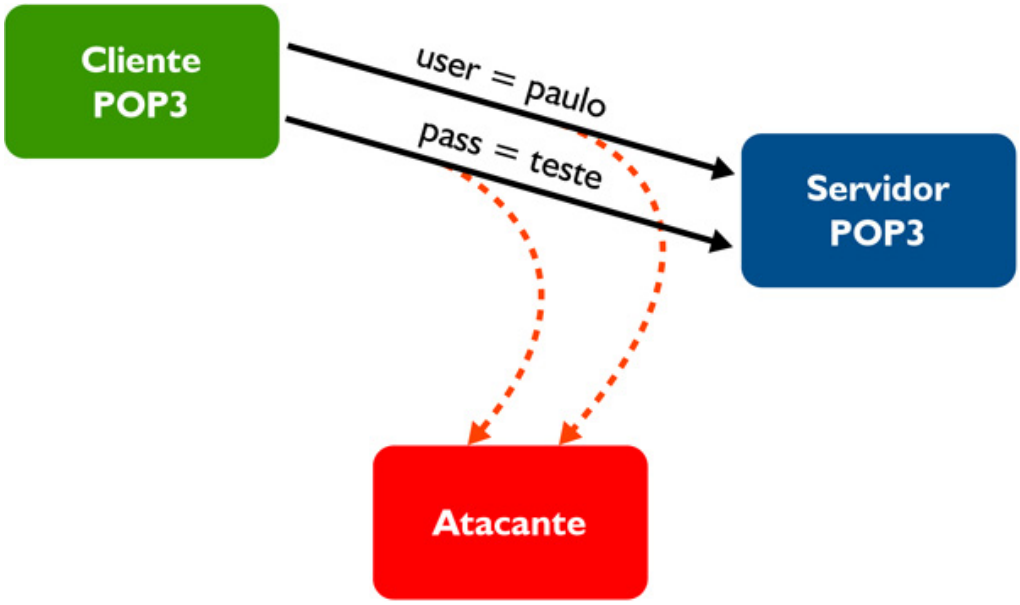
Em ambos os protocolos, esses novos mecanismos estão relacionados, principalmente, à possibilidade de criptografar o trocado entre clientes e servidores.

Vídeo 03 - Problemas de Segurança

POP3 e POP3S

A versão atual do protocolo POP (POP3 ou *Post Office Protocol version 3*) foi padronizada em 1988, oferecendo suporte apenas aos mecanismos básicos de autenticação, como usuário e senha. Nessa versão inicial, também não havia nenhum tipo de suporte à criptografia, ou seja, todos os dados trocados entre clientes e servidores, inclusive usuários, senhas e o conteúdos das mensagens são enviados pela rede de forma "legível" para qualquer atacante interessado em capturar essas informações. A **Figura 1** ilustra um atacante capturando usuários e senhas do serviço POP3.

Figura 01 - Atacante capturando usuários e senhas do serviço POP3.



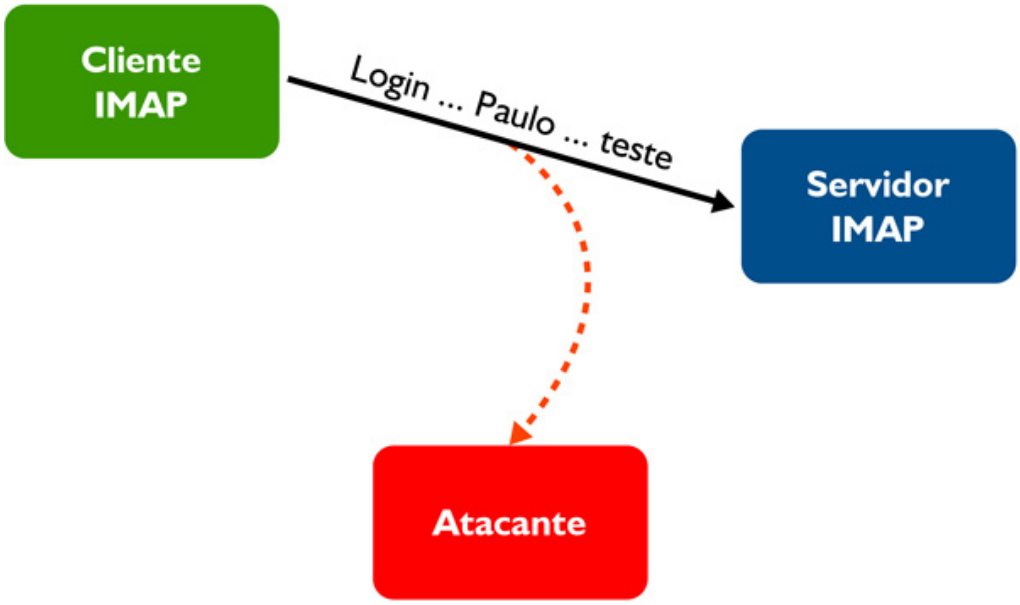
Novas funcionalidades vêm sendo inseridas no POP3 original ao longo dos anos. Dentre elas podemos destacar o uso de mecanismos de autenticação mais avançados e, principalmente, o uso de criptografia. Existem duas formas básicas de se utilizar criptografia juntamente com o serviço de POP3, uma delas é o SSL (*Security Sockets Layer*), que você estudou na Aula 10 desta disciplina. A outra forma provê criptografia na camada de transporte, sendo conhecida como TLS (*Transport Layer Security*). Normalmente, os clientes e servidores oferecem suporte às duas formas de criptografia. É importante destacar que o protopolo POP original permanece inalterado, no entanto, agora, as mensagens trocadas entre clientes e servidores são criptografadas.

Dessa forma, o atacante da **Figura 1** não conseguirá "ler" os dados trocados entre o cliente e o servidor, mesmo que os intercepte. O POP3 com criptografia é comumente chamado de POP3S e utiliza uma porta TCP distinta (995 ao invés de 110) do POP3 original.

IMAP e IMAPS

Um cenário semelhante ao da **Figura 1** é mostrado na **Figura 2**. No entanto, agora, cliente e servidor utilizam o protocolo IMAP. De forma semelhante ao POP3, o IMAP (atualmente na versão 4, padronizada em 2003) não realiza, por padrão, nenhum tipo de criptografia, e o atacante novamente consegue capturar e entender as mensagens trocadas entre cliente e servidor.

Figura 02 - Atacante capturando usuários e senhas do serviço IMAP.



As formas de se utilizar criptografia juntamente com o serviço de IMAP são semelhantes às utilizadas pelo POP3, sendo elas o SSL (*Security Sockets Layer*) e o TLS (*Transport Layer Security*). Novamente, caso se utilize criptografia, um possível atacante que capture a troca de mensagens entre cliente e servidor IMAP não conseguirá ler o conteúdo delas. O IMAP com criptografia é comumente chamado de IMAPS e utiliza uma porta TCP distinta (993 ao invés de 143) do IMAP original.

Atividade 02

1. Por que POP3S e IMAPS não são considerados novos protocolos?

Segurança no Envio de E-mails

No envio de mensagens eletrônicas, utiliza-se o protocolo SMTP, tanto na comunicação entre clientes e servidores, como entre os servidores de origem e destino da mensagem. Na disciplina de Redes de Computadores, você estudou como é simples o procedimento de envio de uma mensagem, podendo isso ser feito, simplesmente, conectando-se diretamente na porta 25 do servidor SMTP de origem e digitando os comandos apropriados. Isso se deve ao fato do protocolo SMTP original não possuir nenhuma preocupação com autenticação de usuários ou

segurança das mensagens enviadas e recebidas por um servidor. Historicamente, essas fraquezas do SMTP têm sido amplamente exploradas por atacantes, notadamente para o envio de SPAMS.

Curiosidade!

No decorrer da disciplina de segurança, você aprendeu que sniffers são *softwares* capazes de capturar todo o tráfego que chega ou sai de uma máquina ou rede. Contudo, também existem alguns sniffers com finalidade específica, sendo um dos mais conhecidos o dsniff, disponível em http://www.monkey.org/~dugsong/dsniff/. Com ele é possível capturar, exclusivamente, os nomes de usuários e senhas enviados por protocolos que não utilizam criptografia, como o POP3 e IMAP.

Segurança na Comunicação entre Clientes e Servidores SMTP

De forma semelhante aos protocolos de leitura de e-mail, que evoluíram de forma a tornar a comunicação entre clientes e servidores segura, o protocolo SMTP recebeu uma série de extensões de segurança, que permite realizar a autenticação dos usuários que utilizam o servidor, bem como a criptografia dos dados enviados e recebidos.

Tornar a autenticação obrigatória é uma funcionalidade diretamente relacionada ao bloqueio de SPAMS, dado que apenas usuários, ou seja, clientes de e-mail autenticados conseguirão enviar emails por aquele servidor. Dessa forma, mesmo que uma máquina da rede interna de uma empresa esteja infectada com um vírus ou ferramenta de envio de SPAMS, ela não terá sucesso, a menos que conheça as credenciais (usuário e senha), utilizadas por algum usuário daquele servidor.

Já a possibilidade de criptografar os dados trocados tem importância semelhante àquela estudada para o POP3S e IMAPS: evitar que atacantes ou qualquer outra pessoa mal intencionada consiga capturar e ler o conteúdo das mensagens trocadas entre clientes e servidores.

O protocolo de envio de mensagens entre cliente e servidores SMTP, utilizando os mecanismos de segurança, é popularmente chamado de SMTPS e utiliza a porta TCP 465 (também se utiliza a porta TCP 587, exclusivamente para o envio de mensagens de clientes autenticados). De forma semelhante ao POP3S e IMAPS, o SMTPS define uma série de mecanismos de autenticação e, para criptografia, pode utilizar SSL ou TLS (sem alterar o protocolo SMTP original).

Vídeo 04 - Mecanismos de Segurança

Atividade 03

1. Por que o uso de mecanismos de segurança na comunicação entre clientes e servidores SMTP pode diminuir o número de SPAMS?

Segurança na Comunicação entre Servidores SMTP

Existem diversos aspectos importantes a serem considerados na comunicação direta entre servidores SMTP, contudo, em nossa aula, iremos nos concentrar em uma série de técnicas atualmente utilizadas para tentar coibir o envio de SPAMS.

Block Lists

É uma das formas mais antigas e simples de filtragem de SPAMS que funciona pela inserção, na configuração do servidor de correio, de uma listagem de endereços IP ou domínios "proibidos". Caso se receba uma mensagem de um dos domínios ou endereços listados, ela será automaticamente descartada.

A manutenção manual da lista de bloqueios seria uma tarefa bastante trabalhosa, contudo, existem várias listas disponíveis na internet, sendo que, no Brasil, a mais famosa é disponibilizada em <http://malware.com.br/lists.shtml>.

Greylisting

É um método utilizado por servidores SMTP por meio do qual cada servidor "rejeita temporariamente" mensagens vindas de qualquer origem não conhecida. O conceito de funcionamento do *greylist* é simples:

- Ao receber a primeira mensagem de um local (IP ou domínio) não conhecido, o servidor de correio responde com um erro não fatal, informando à origem que ela deve tentar enviar novamente a mensagem após algum tempo.

- Assume-se que, caso a origem seja um servidor legítimo (e não um vírus ou outra ferramenta qualquer de envio de SPAMS), ele, realmente, irá tentar reenviar a mensagem após algum tempo. Caso isso ocorra, a mensagem será aceita pelo servidor de destino (bem como as subsequentes vindas dessa mesma origem).

- Assume-se, também, que, caso a origem seja um vírus ou outra ferramenta de envio de SPAMS qualquer, ela não irá tentar reenviar mensagens em caso de erros. Isso realmente ocorre na maioria dos casos.

A principal vantagem do *greylisting* é que sua configuração é extremamente fácil e adiciona pouco processamento extra no servidor SMTP. A principal desvantagem é que sempre será inserido um grande atraso no recebimento da primeira mensagem de cada domínio ou IP desconhecido, podendo ele variar de alguns minutos até algumas horas.

Sender Policy Framework

É uma técnica que possibilita aos administradores especificar quais servidores estão habilitados a enviar e-mail a partir de um domínio. Sua implementação é dependente do serviço de DNS, pela inserção de registros específicos (tipo SPF) nas zonas de DNS.

Ao receber um e-mail de um domínio qualquer, um servidor SMTP pode checar se ele vem de um endereço IP autorizado. Caso positivo, a mensagem será aceita; caso contrário, ele será descartado.

Softwares antispam e antivírus

Os *softwares* de antispam e antivírus são, normalmente, utilizados como a última e mais complexa linha de defesa de servidores SMTP no combate aos SPAMS. Normalmente, os *softwares* de antispam realizam uma série de verificações no conteúdo de cada mensagem para decidir se essa é ou não um SPAM. Para realizar a verificação, os *softwares* antispam devem possuir e manter atualizada uma grande base de dados de "assinaturas" de mensagens que são, conhecidamente, SPAMS. Cada mensagem a ser analisada é comparada com a base de assinaturas e, dependendo de seu grau de semelhança, ela será ou não considerada um SPAM. Essa técnica é semelhante à utilizada pelos *softwares* de antivírus que tentam detectar a existência de vírus, worms, cavalos de Tróia etc. em arquivos anexados às mensagens. Na prática, esses dois *softwares* são, normalmente, utilizados em conjunto.

A principal vantagem dos *softwares* de antispam e antivírus reside no fato de que, quando bem configurados, eles realizam um nível de detecção de SPAMS excelente. Entre suas desvantagens destacamos a possibilidade da ocorrência de falsos positivos (onde mensagens legítimas são classificadas como SPAMS) e o fato de necessitarem de muitos recursos extras, de processamento e memória, no servidor que os executa.

Vale salientar que, na prática, grandes empresas e instituições irão se utilizar de uma combinação de todos os mecanismos aqui descritos (além de outros não vistos) para a detecção de SPAMS.

Atividade 04

Pesquise

1. Gostou do tema? Então, pesquise mais sobre ele no site http://www.antispam.br/ e elabore um texto sobre Spams.

Resumo

Nesta aula, você aprendeu mais sobre diversas técnicas utilizadas para trazer segurança ao serviço de e-mail. Os protocolos para leitura de e-mail como POP3 e IMAP evoluíram para versões mais seguras, que utilizam SSL ou TLS para permitir a criptografia dos dados trocados entre clientes e servidores. Uma evolução semelhante pode ser observada na comunicação entre clientes e servidores do protocolo SMTP. Na comunicação entre servidores SMTP, estudamos uma série de técnicas que tentam mitigar o envio e recebimento de SPAMS, são elas: *block lists*, *greylisting*, *Sender Policy Framework* e os *softwares* antispam e antivírus.

Autoavaliação

1. Por que a criptografia é importante para os usuários dos protocolos POP3 e IMAP?

2. Quais as principais desvantagens de se utilizar o mecanismo de greylisting no tratamento de SPAMS?

3. Marque Verdadeiro ou Falso nas assertivas a seguir:

   ( ) Os serviços de POP3 e IMAP sempre tiveram mecanismos básicos de autenticação.
   ( ) A comunicação entre clientes e servidores SMTP é sempre autenticada.
   ( ) Block lists são a forma mais moderna e aprimorada para detectar SPAMS.
   ( ) O Sender Policy Framework funciona com base no serviço de DNS.
   ( ) O funcionamento dos softwares antispam é bastante leve na detecção de SPAMS.

Referências

IMAP and POP3. **Building a Mail Server with Courier and Cyrus, No Starch Press**. 2008.

KUROSE, James F.; ROSS, Keith W. **Redes de Computadores e a Internet**. São Paulo: PEARSON EDUCATION, 2010.