Congresso Internacional de Administração
Gestão Estratégica na Era do Conhecimento
de 08 a 12 de Setembro de 2008 - Ponta Grossa - PR

Autenticação IEEE 802.1x em Redes de Computadores Utilizando TLS e EAP

Luiz Gustavo Barros (UEPG) luizgb@uepg.br
Dierone César Foltran Junior (UEPG) foltran@uepg.br

Resumo:
As tecnologias de redes de computadores sem fio hoje estão entre as mais utilizadas devido a sua facilidade de uso, comodidade e flexibilidade. Porém como este meio de acesso é compartilhado, diversos métodos de criptografia e segurança são oferecidos para garantir que somente usuários legítimos tenham acesso aos recursos da rede. Uma forma de se obter essa legitimidade do usuário é implementar a autenticação IEEE 802.1x utilizando TLS e EAP para o uso de certificados digitais sendo estes integrados a um diretório LDAP onde se encontram todas as contas de usuários. Assim é possível identificar cada usuário, definir quais recursos estão disponíveis a ele e inibir acessos indevidos e não autorizados.
Palavras-chave: Redes de Computadores, Autenticação IEEE 802.1x, Redes sem fio, Certificação Digital.

1. Introdução

Durante os últimos anos as redes de computadores tiveram um grande crescimento principalmente devido a popularização da Internet (NICBR, 2006). Entretanto, a infra-estrutura de redes de computadores necessita de atualizações para suportar novos protocolos para permitir seu gerenciamento e controle sobre os usuários da mesma.

Em um ambiente de rede onde o meio de acesso é compartilhado e aberto, como nas redes sem fio ou no caso das redes cabeadas que existam segmentos da mesma que não possam ser verificados, a confiança nos *hosts* fica limitada. Para contornar esses aspectos falhos de segurança mencionados acima existem diversos métodos disponíveis para implementação. Uma forma eficiente é prover um mecanismo de segurança através de um protocolo que ofereça opções de segurança confiáveis.

Desta forma, o padrão IEEE 802.1x é o que provê autenticação entre os clientes da rede e o ativo no qual os mesmos estão conectados podendo este ser um *switch* ou um ponto de acesso (AP - *Access Point*) para acessos sem fio.

Portanto, o padrão IEEE 802.1x descreve um modelo de controle de acesso à rede e uma arquitetura de controle centralizada que se integra com o padrão AAA (*Authentication, Authorization and Accounting*) da IETF (*Internet Engineering Task Force*) definido em (VOLLBRECHT, 2000).

Neste estudo será proposta uma arquitetura utilizando certificados digitais para o processo de autenticação, um diretório LDAP (*Lightweight Directory Access Protocol*) para armazenar os dados dos usuários no processo de autorização e um servidor RADIUS (*Remote Authentication Dial In User Service*) para a contabilização dos acessos. O RADIUS também irá prover a interoperabilidade dos dois primeiros processos com este último, utilizando um

módulo EAP (*Extensible Authentication Protocol*) com suporte ao protocolo TLS (*Transport Layer Security*) para a identificação e validação do certificado digital fornecido pelo cliente. Será definido um ambiente de experimentação desta arquitetura utilizando uma rede sem fio com clientes móveis.

2. O padrão AAA

Em segurança da informação, o padrão AAA é uma referência aos protocolos relacionados com os procedimentos de autenticação, autorização e contabilização *(accounting)*. A autenticação verifica a identidade digital do usuário de um sistema, a autorização garante que um usuário autenticado somente tenha acesso aos recursos autorizados e, por fim, a contabilização refere-se a coleta de informações sobre o uso dos recursos de um sistema pelos seus usuários.

No processo de autenticação, é necessária a reciprocidade. O usuário tem que possuir a certeza de que está enviando as suas informações de conta para o local correto. Um usuário deve identificar-se e autenticar-se para o sistema, mas o sistema não se autentica para o usuário de maneira óbvia. O problema é simplesmente composto pela crescente quantidade de vulnerabilidades no pacote de protocolos TCP/IP, que pode criar informações incorretas para vantagem de um usuário que esteja tentando obter acesso indevido a um recurso da rede.

Para solucionar este problema, conhecido como *man-in-the-middle*, definido em (ASOKAN, 2005), é preciso colocar um mecanismo adequado de autenticação mútua. Autenticação mútua é quando o *host* autentica o cliente e o cliente autentica o *host*. Os métodos de autenticação mútua são baseados em uma infra-estrutura de chave pública (PKI – *Public Key Infrastructure*). A norma RFC 2716 (ABOBA, 1999) define o protocolo EAP utilizando TLS este que será o objeto de estudo deste trabalho.

O procedimento de autorização é a concessão de tipos específicos de serviços para um usuário, com base na sua autenticação, quais serviços estão sendo solicitados, bem como o atual estado do sistema. A autorização pode ser baseada em restrições como, por exemplo, hora, localização física ou contra várias sessões simultâneas pelo mesmo usuário. A autorização determina a natureza do serviço, que é concedido a um usuário. Exemplos de tipos de serviços incluem, filtragem de endereço IP, concessão de endereço IP, concessão de rotas, QoS (*Quality of Service*), serviços de controle de largura de/gestão de tráfego e criptografia entre outros (VOLLBRECHT, 2000).

O processo de contabilização (*accounting*) refere-se ao monitoramento do consumo de recursos de rede pelos usuários. Estas informações poderão ser utilizadas para o gerenciamento, planeamento, pagamento ou para outros fins. Accounting em tempo real refere-se à informação que é entregue simultaneamente com o consumo dos recursos. Accounting em batch refere-se à informação que é armazenada até que seja utilizada em momento oportuno. Informações típicas que são recolhidas no processo de accounting é a identidade do usuário, a natureza do serviço, quando o serviço foi concedido e quando o mesmo foi encerrado.

Os procedimentos acima que compõem a arquitetura AAA são necessários para oferecer uma forma de autenticação segura a uma rede onde é necessário ter controle sobre a forma de acesso dos usuários.

3. Redes sem Fio

O IEEE, em 1999, definiu uma norma para redes locais sem-fio chamada "*Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications*" (IEEE, 1999).

O padrão IEEE 802.11, como todos os protocolos da família 802.x, especifica as camadas física e de controle de acesso ao meio (MAC).

Assim, as redes de padrão IEEE 802.11, conhecidas também por como *Wi-Fi - Wireless Fidelity*, utilizam como meio físico ondas de rádio para a transmissão de dados. Dessa forma, para dois computadores se comunicarem com a ausência de fios é necessário apenas que estes placas de rede padrão *Wi-Fi*.

O conjunto básico de serviços *(*BSS - *Basic Service Set*) é o bloco fundamental de construção da arquitetura do padrão IEEE 802.11 (IEEE, 1999). Um BSS é definido como um grupo de estações que estão sobre o controle direto de uma única função de coordenação, que determina quando uma estação pode transmitir e receber dados (RUBINSTEIN, 2002).

No protocolo IEEE 802.11 existem dois tipos de redes sem fio: *ad-hoc* ou infra-estruturada. Uma rede *ad-hoc* é composta somente por estações dentro de um mesmo BSS que se comunicam entre si sem a ajuda de uma infra-estrutura. Qualquer estação pode estabelecer uma comunicação direta com outra estação no BSS sem a necessidade que a informação passe por um ponto de acesso centralizado (CROW, 1999). O padrão 802.11 refere-se a uma rede *ad-hoc* como um BSS independente. Já em uma rede infra-estruturada, é utilizado um ponto de acesso que é responsável por quase toda a funcionalidade de rede.

O padrão IEEE 802.11 também tem como objetivo especificar os detalhes da camada física e da subcamada MAC da camada de enlace para redes de computadores sem fio (WLAN - *Wireless Local Area Network*), tendo como fim relacionar as diferenças existentes com as redes *Ethernet*, tornando-as interoperáveis (DUARTE, 2003).

4. LDAP - Lightweight Directory Access Protocol

A necessidade de integração de informações de maneira clara e consistente, de forma a reduzir o custo de sua manutenção motivou o surgimento de um padrão que provesse tais características. Assim, o padrão LDAP foi criado com esse intuito e trata-se de um protocolo que define um método para o acesso e a atualização de informações em um diretório. A definição de um diretório descreve um banco de dados especializado em leitura apenas e não em gravação.

Portanto, o LDAP define um protocolo de comunicação desenvolvido para rodar sobre a pilha de protocolos TCP/IP. Assim, o mesmo define o transporte e o formato das mensagens utilizadas pelo cliente para acessar os dados que estão armazenados em um diretório do tipo X.500.

É através do padrão X.500 que se organizam as entradas do diretório em um espaço de nomes hierárquico (uma árvore) capaz de incorporar grandes volumes de informação. A árvore de diretório pode ser criada de acordo com a necessidade. O LDAP também define métodos de busca para tornar a recuperação dessa informação de forma eficiente (BARTH, 2006).

Entretanto, o LDAP não define o serviço de diretório em si. Com o LDAP, o cliente não é dependente da implementação em particular do serviço de diretório que está no servidor.

5. Padrão IEEE 802.1x

O IEEE 802.1X é o padrão adotado para autenticação, ao nível de porta, em redes IEEE 802 cabeadas ou sem fio, atendendo à arquitetura AAA. O padrão define porta como

sendo um ponto de conexão à LAN, podendo ser uma porta física, em redes cabeadas, ou uma porta lógica, como no caso da associação entre um dispositivo sem fio e o ponto de acesso.

O padrão IEEE 802.1x é uma solução para os problemas de autenticação encontrados no IEEE 802.11, pois o mesmo tem suporte a diversos métodos de autenticação existentes.

Desta maneira, o IEEE 802.1x garante compatibilidade entre o Protocolo de Integridade Temporal de Chave (TKIP - *Temporal Key Integrity Protocol*), que foi desenvolvido para solucionar o problema de chave estática do WEP, e o Padrão de Criptografia Avançada (AES - *Advanced Encryption Standard*), que é um mecanismo forte de criptografia que vem sendo adotado recentemente.

Uma forma de utilizar os recursos que o padrão IEEE 802.1x oferece, é implementar o protocolo EAP (BLUNK, 1998), proposto para ampliar a funcionalidade de autenticação do protocolo ponto-a-ponto (PPP - *Point-to-Point Protocol*) (SIMPSON 1994), antes limitada aos mecanismos providos pelo Protocolo para Controle de Link (LCP - *Link Control Protocol*), que eram o Protocolo de Autenticação por Senha (PAP - *Password Authentication Protocol*) e o Protocolo de Autenticação por Negociação de Desafio (CHAP - *Challenge Handshake Authentication Protocol*) (SIMPSON, 1996). O PAP é um protocolo utilizado principalmente para autenticação em redes discadas, no qual o login e a senha trafegam em texto claro. O CHAP provê criptografia somente do usuário e senha, porém os dados também trafegam em texto claro.

Utilizando o EAP é possível ter independência de mecanismos de autenticação PPP, sendo assim uma alternativa interessante para interligação de redes visto a sua capacidade de adaptação a novos mecanismos. Neste trabalho será utilizado o EAP em conjunto com o protocolo TLS utilizando certificados digitais para autenticação dos usuários.

Uma vantagem do uso do protocolo EAP é o aumento de vida útil dos equipamentos que possuem suporte ao protocolo IEEE 802.1x, pois os mesmos passam a funcionar como intermediários entre o *host* cliente e o servidor de autenticação, não sendo necessário implementar mecanismos adicionais de segurança no próprio equipamento.

6. Protocolo RADIUS - Remote Authentication Dial In User Service

O RADIUS é um protocolo utilizado para disponibilizar acesso a redes utilizando a arquitetura AAA. Inicialmente foi desenvolvido para uso em serviços de acesso discado. Atualmente é também implementado em pontos de acesso sem fio e outros tipos de dispositivos que permitem acesso autenticado a redes de computadores. O protocolo RADIUS é definido pela RFC 2865 (RIGNEY, 2000).

O RADIUS foi idealizado para centralizar as atividades de Autenticação, Autorização e Contabilização. O processo de autenticação funciona da seguinte maneira: um *host* faz uma requisição de acesso a um cliente RADIUS (um ponto de acesso sem fio, por exemplo). Este cliente requisita as credenciais e os parâmetros da conexão ao *host* de origem e os envia na forma de uma mensagem RADIUS, ao servidor. Este servidor checa os dados enviados e autentica e autoriza a requisição do cliente RADIUS. Sendo o acesso autorizado ou negado, uma mensagem é retornada ao cliente. No caso de acesso autorizado, o cliente libera o acesso à rede ao *host* que fez a requisição de acesso. A Figura 1 exemplifica esse processo.

Figura 1 - Processo de autenticação e autorização RADIUS

É importante ressaltar que toda a comunicação entre o *host* e o cliente RADIUS é realizada na camada de enlace do modelo OSI. Entre o cliente e o servidor RADIUS, a comunicação se dá na camada de aplicação. Somente após o acesso ser autorizado ao *host* que a o mesmo tem acesso concedido à camada de rede e superiores.

Em relação à segurança, pela RFC 2865 (RIGNEY, 2000), não é necessário que as requisições de acesso RADIUS sejam autenticadas e protegidas em relação à integridade. Já na RFC 2869 (RIGNEY, 2000) define-se que todas as mensagens envolvidas em uma conversação EAP incluam autenticação e proteção à integridade.

7. Ambiente de Experimentação

O ambiente de experimento é compreendido pela área da Universidade Estadual de Ponta Grossa (UEPG), em seus dois campus localizados em Ponta Grossa, o campus Central e o campus Uvaranas.

De início foi criada uma autoridade certificadora (AC) raiz denominada Universidade Estadual de Ponta Grossa, é através dela que todos os certificados digitais são emitidos, bem como autoridades certificadoras intermediárias. Adicionalmente foi criada uma AC subordinada a AC UEPG raiz, denominada Autoridade Certificadora UEPG v1, para melhor organizar os certificados. Sendo assim, esta última foi destinada a emitir certificados para os usuários do diretório LDAP que já se encontrava implementado na Universidade desde abril de 2007 e que contém todas as contas de usuários da instituição. O diretório LDAP na UEPG serve provê autenticação de contas de e-mail e autenticação de usuários para navegação via servidor *proxy* da Universidade.

Os usuários da rede da Universidade devem requisitar seus próprios certificados através de um sistema que autentica os mesmos e envia o certificado digital para o seu respectivo e-mail institucional. O sistema permite após a primeira requisição, recuperar o certificado pessoal, recuperar a senha do certificado, bem como revogar o certificado em caso de extravio ou perda. Um certificado digital pessoal é mostrado na figura 2.

Figura 2 – Certificado digital pessoal

O processo de autorização no servidor RADIUS é o de validação do certificado, que já foi descrito anteriormente. A autenticação é feita no diretório LDAP. Uma vez com o atributo nome de usuário do certificado digital, é feita uma pesquisa no diretório por esse usuário.

O fluxograma do processo de autorização e autenticação é descrito na Figura 3. O *host* envia uma requisição de acesso a um cliente RADIUS, comumente, um ponto de acesso sem fio. O cliente pede as credenciais para o *host.* A credencial utilizada no nosso experimento é o certificado digital. Assim, o cliente repassa as credenciais para o servidor RADIUS. O mesmo a usa para fazer uma pesquisa no diretório LDAP e verificar se a mesma é válida para autenticação. Se afirmativo, o servidor RADIUS prossegue com a validação do certificado digital, realizando a operação de autorização. Se o certificado digital não tiver nenhuma restrição quanto à autorização, o servidor RADIUS autoriza a conexão e o cliente RADIUS libera a mesma para o *host* que fez a requisição inicial.

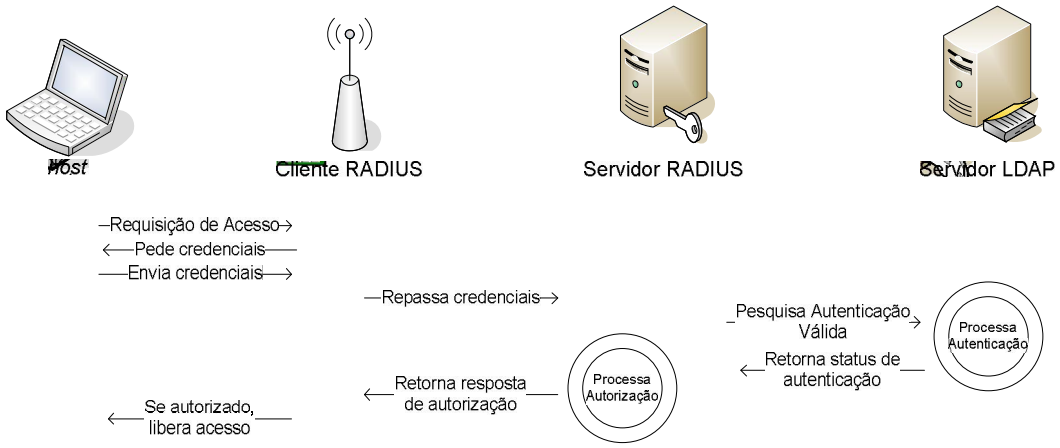

Figura 3 - Fluxograma do processo de autorização e autenticação

Os equipamentos utilizados para este experimento foram pontos de acesso sem fio marca Linksys modelo WRT54G com seu *firmware* modificado. A modificação do *firmware* se deve a maior estabilidade do *firmware* modificado, se comparado ao original e devido também a presença de alguns recursos adicionais necessários não disponíveis inicialmente. Os pontos de acesso foram distribuídos em diversos locais da Universidade, abrangendo os locais de maior concentração de estações móveis.

8. Conclusão

Utilizar um ambiente de rede que possui uma forma de autenticação e autorização para acesso ao meio é uma das formas de aumentar a segurança. Com o processo de autorização, somente usuários legítimos e devidamente identificados tem acesso aos recursos disponíveis. Já o processo de autorização fornece flexibilidade para implementar uma hierarquia de acesso, bem como manter centralizada a base de usuários. Utilizar um meio de contabilizar o acesso individual de cada cliente também ajuda no aspecto da segurança, pois é possível definir limites como horários disponíveis para uso e tempo máximo de conexão, por exemplo.

A necessidade da Universidade Estadual de Ponta Grossa em oferecer um acesso sem fio para sua comunidade interna se tornou viável recentemente. E oferecer esse acesso utilizando todos os componentes disponíveis para atingir um nível de segurança onde cada acesso seja individualizado foi o objeto desse estudo.

9. Trabalhos Futuros

Uma vez consolidada a autoridade certificadora e distribuídos certificados digitais pessoais, é possível implementar uma VPN (V*irtual Private Network*) sobre o protocolo IPSec, para oferecer acesso remoto a rede da Universidade, uma vez que parte da infra-estrutura necessária já se encontra pronta.

Outra forma de implementar acesso remoto utilizando parte da infra-estrutura utilizada nesse trabalho seria utilizar o servidor RADIUS também em conjunto com outros tipos de clientes e não somente pontos de acesso sem fio. Para autenticar conexões discadas, o procedimento seria exatamente o mesmo, e o cliente RADIUS seria um RAS (*Remote Access Service*) com modems digitais ligados a linhas telefônicas. É também possível, ainda, estender o uso do protocolo RADIUS para redes com fios, sendo necessária exatamente a mesma forma de autenticação implementada nesse estudo, utilizando *switches* gerenciáveis como clientes RADIUS.

Referências

ABOBA, B.; SIMON D. **RFC 2716 - PPP EAP TLS Authentication Protocol.** 1999.

AKOSAN, N.; NIEMI, V.; NYBERG, K. **Man-in-the-Middle in Tunnelled Authentication Protocols.** 2005, Artigo Científico. *In* 11th Security Protocols Workshop.

BARTH, D.; SIEWERT, V. **Lightweight Directory Access Protocol.** Florianópolis, 2005. Artigo Científico. Serviço Nacional de Aprendizado Industrial – Santa Catarina.

BLUNK, L.; VOLLBRECHT, J. **RFC 2284 - PPP Extensible Authentication Protocol (EAP)**, 1998.

CROW B. *et al*. **IEEE 802.11 wireless local area networks.** 1997. Artigo Científico. *In IEEE Communications Magazine*, vol. 35, n 9, pag. 116-126.

DUARTE, L. **Análise de Vulnerabilidades e Ataques Inerentes a Redes Sem Fio 802.11x.** 2003. Monografia. Universidade Estadual Paulista Júlio de Mesquita Filho, São José do Rio Preto.

IEEE - Institute of Electrical and Electronics Engineers. **Wireless LAN medium access control (MAC) and physical layer (PHY) specifications**. Padrão IEEE 802.11, 1999.

NIC.BR - Núcleo de Informação e Coordenação do Ponto br. **NIC.br anuncia resultados da pesquisa sobre o uso da internet no Brasil.** 2006.

RIGNEY, C. *et al*. **RFC 2865 - Remote Authentication Dial In User Service (RADIUS)**, 2000.

RIGNEY, C.; WILLATS, W.; CALHOUN, P.; **RFC 2869 - RADIUS Extensions**, 2000

RUBINSTEIN M.; REZENDE J. **Qualidade de Serviço em Redes 802.11**. In XX Simposio Brasileiro de Redes de Computadores, 2002.

SIMPSON, W. **RFC 1994 - PPP Challenge Handshake Authentication Protocol (CHAP)**, 1996.

SIMPSON, W. **RFC 1661 - The Point-to-Point Protocol (PPP)**, 1994

VOLLBRECHT, J. et al. **RFC 2904 - AAA Authorization Framework**, 2000.