IEEE 802.11i - Segurança em Redes Wireless

(João Leonardo Martins, Mateus Araújo, Nelson Alves e Paula Grando)

A segurança na transmissão de dados é essencial em todas as áreas do setor de telecomunicações. Porém este assunto se torna mais importante quando qualquer pessoa consegue ter acesso ao meio de transmissão, como no caso das redes *wireless*.

Embora o primeiro padrão adotado (802.11) previa o uso de autenticação e segurança no enlace com o protocolo WEP, este se mostrou ineficiente devido a fragilidade da criptografia e das sucessivas formas de ataques para burlar esta segurança. O documento 802.11i definiu um conjunto de protocolos e padrões relacionados a segurança. Entre esses está o TKIP, que garante uma integridade maior aos dados. Como diferencial deste padrão, está o protocolo CCMP e o algoritmo AES, além de o protocolo de autenticação EAP.

Será abordado o primeiro protocolo WEP e seus problemas, e os protocolos padronizados posteriormente no documento 802.11i, que possibilitaram uma melhoria na integridade e criptografia da rede.

Protocolo WEP

O protocolo WEP utiliza o algoritmo de criptografia RC4, que é composto de uma chave fixa (40 ou 104 bits) mais um vetor de inicialização variável de 24 bits. Como a maior parte da chave é fixa, uma aplicação que identifique os 24 bits (bits esses que podem se repetir num curto período) terá acesso a toda a chave, e consequentemente, à rede.

Também o processo de autenticação é vulnerável, uma vez este vetor de inicialização é repassado do *Acess Point* para o dispositivo, podendo ser capturado este pacote no meio do caminho.

WPA (TKIP)

Com as limitações do protocolo WEP, surge a necessidade de um processo de acesso à rede mais seguro: o WPA, ou WEP2 ou TKIP.

Dentre suas vantagens, podemos destacar: a compatibilidade com versões anteriores e posteriores, e a garantia de integridade, que é possível através do MIC (*Message Integrity Code*). Este campo em suma mitiga ataques *bit flipping*, que basicamente ocorrem através da alteração de informações da criptografia pelo intruso, bastante comum em WEP. Este campo é adicionado ao frame e tem seu valor baseado no MAC do destino e origem, e com estes dados é gerado uma chave (*hashing*), tornando a troca de informações mais seguras.

Também foi inserido ao frame o campo SEQ, de sequência, onde a finalidade é acabar com ataques chamados *replay attack*. Estes ataques ocorrem, por exemplo, quando o atacante consegue determinada informação e com essa informação tenta se passar por outro dispositivo. Com a inserção do SEQ, isso torna-se mais difícil, pois traz a ideia de sessão, onde finalizada a troca de informações, a sessão é terminada e mesmo sabendo parte da informação, se houver a tentativa de invasão com um número de SEQ já utilizado pelo interlocutor, a solicitação é negada.

AES/CCMP

O protocolo CCMP utiliza o algoritmo AES, que possui chaves de 128, 192 e 256 bits. Este protocolo utiliza combinações entre o bloco de dados e a chave de criptografia, fazendo com que toda nova combinação dependa do resultado do antecessor para continuar. Isto dificulta a obtenção preemptiva da chave, além de, como o Vetor de inicialização possuir 48 bits(que é utilizado no primeiro passo pois ainda nao tem texto anterior cifrado), haver uma gama maior de combinações.

EAP

O protocolo 802.11i implementa o padrão 802.1x, que é utilizado para autenticação, controle de acesso e distribuição de chaves criptográficas. Neste padrão, há 3 componentes: um autenticador (em geral o Acess Point), quem deseja se conectar, e um servidor de autenticação. Isto garante mais segurança, pois é necessário passar por um desafio proposto pelo servidor (senha de autenticação), para só depois ser trocadas as chaves criptográficas do TKIP/AES.

Referências bibliográficas

Maia, Roberto. **Segurança em Redes Wireless - 802.11i.** Universidade Federal do Rio de Janeiro, 2003. Disponível online em: <http://www.gta.ufrj.br/seminarios/semin2003_1/rmaia/802_11i.html>. Acessado em: 24 de julho de 2016.

Paim, Rodrigo R. **WEP, WPA e EAP.** Universidade Federal do Rio de Janeiro, 2011. Disponível online em: <http://www.gta.ufrj.br/ensino/eel879/trabalhos_vf_2011_2/rodrigo_paim/index.html> Acessado em: 24 de julho de 2016.