Segurança em IEEE 802.11 Wireless LAN

Giovan Carlo Germoglio

Mestrado em Informática
Departamento de Informática
Universidade do Minho

Contextualização

- Padrão IEEE 802.11 Wireless LAN:
  - Estabelecido em 1989;
  - Equivalência com a Ethernet;
  - Apenas transmissão de dados;
  - Atualmente acomoda transmissão de áudio, vídeo e outras formas de multimedia;
  - Exigência de segurança na transmissão dos dados.

O padrão IEEE 802.11 WLAN foi estabelecido em 1989. O que se pretendia originalmente era um novo padrão em que houvesse uma certa equivalência com o padrão já existente Ethernet. Na concepção desse novo padrão, pensava-se apenas na transmissão de dados, porém hoje pode-se perceber sua utilização na transmissão de áudio, vídeo e outras formas de multimedia. Não só para esse padrão como para qualquer outro existente ou que venha a existir, sempre se exigirá um determinado nível de segurança.

Contextualização

- Diferença entre Wired e Wireless:
  - Acesso ao dado transmitido;
  - Meio físico X Ar;
    - Acesso por equipamentos simples;
  - Grande foco na segurança;
  - Abordagem do protocolo de segurança, suas falhas e soluções propostas.

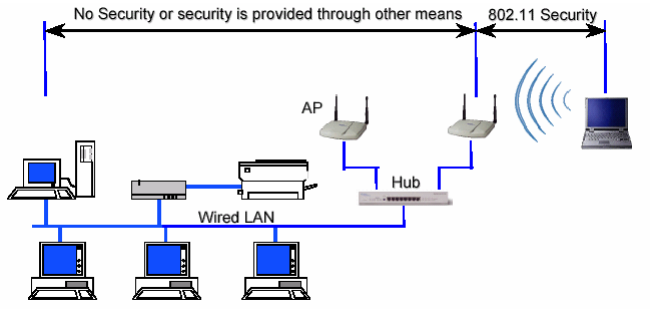
O principal aspecto que difere uma rede Wireless de uma rede Wired está relacionado ao meio utilizado para transmissão dos dados. Enquanto uma rede Wired utiliza os diversos meios físicos existentes para transmissão dos seus dados, como: cabos coaxias, par-transados, fibra ótica, etc; nas redes Wireless, estão ausentes quaisquer desses meios para transmissão, utilizando-se apenas o ar para o fluxo das informações. Como essa abordagem torna mais vulnerável o acesso aos dados por indivíduos não autorizados, houve e ainda há um grande foco no aspecto da segurança.

Segurança da 802.11 WLANs

- Serviço de Segurança WEP – Wired Equivalent Privacy;
- Proteção durante a transmissão:
  - Proteção entre clientes e APs;
- Não faz proteção fim-a-fim.

Com esse grande preocupação relacionada à segurança, o padrão IEEE 802.11 foi concebido juntamente com o protocolo WEP – Wired Equivalent Privacy. O protocolo de segurança WEP atua entre os clientes móveis ou mobile node e os APs – Access Point, não fazendo a proteção dos dados fim-a-fim, ou seja, desde o nó emissor até o nó receptor.

WEP - Segurança da 802.11 WLANs



Segurança da 802.11 Wireless LAN em uma rede típica [1]

Figura demonstrando a explicação dada anteriormente.

WEP - Segurança da 802.11 WLANs

- Características do serviço de segurança:
  - 1° - Authentication:
    - Verifica a identidade do Mobile Node.
  - 2 ° - Confidentiality ou privacy:
    - Tenta manter a mesma privacidade alcançada em redes normais.
  - 3 ° - Integrity:
    - Assegura que a mensagem não foi modificada.

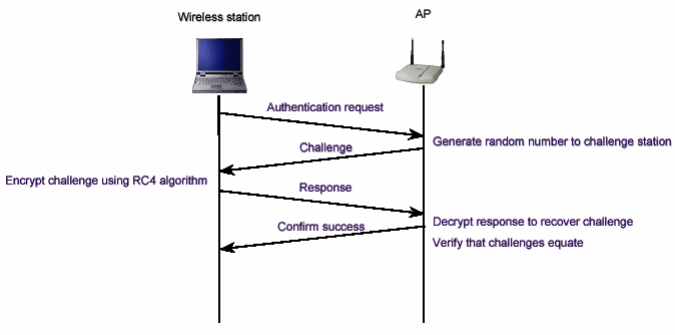
O protocolo WEP possui três características fundamentais, que são: autenticação, a fase onde se verifica a identidade do mobile node; a privacidade, procura manter seguro os dados que serão transmitidos; e a integridade, onde é assegurada a autenticidade do dado transmitido.

Authentication

- Duas formas de validação dos wireless users:
  - Open-System Authentication:
    - Não baseada em criptografia;
    - Não há verificação de identidade;
    - Autenticação com apenas troca de mensagens.
  - Shared-Key Authentication:
    - Baseado numa resposta a um convite;
    - Conhecimento de um shared-secret;
    - Algoritmo utilizado RC4.

Nas redes wireless, a autenticação pode ser realizada de duas formas: a primeira seria através do Open-System Authentication, onde não há criptografia dos dados, não existe a verificação da identidade do mobile node, pois a autenticação é feita apenas com o envio do endereço MAC do MN; o segunda forma seria através da Shared-Key Authentication, utilizando-se um algoritmo RC4 para cifragem dos dados, tanto o MN como o AP tem que ter o conhecimento de uma shared-secret.

Authentication



Mensagem de autenticação com a shared-Key [1]

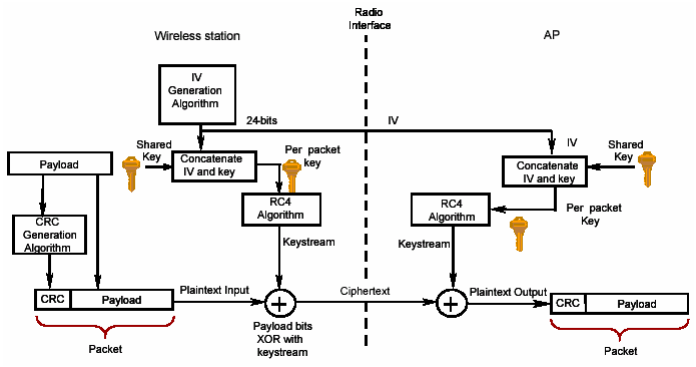
Esquema que exemplifica o funcionamento da utilização da Shared-key Authentication.

Confidentiality ou privacy

- Garantida através de técnicas de criptografia;
- RC4 symmetric-key;
- XOR entre os dados e a Key Stream;
  - Concatenação da Shared-key e a private-key.
- Aplicação do WEP em todas as camadas acima da 802.11 WLAN;
- Shared-key de 24 bits.

A privacidade dos dados transmitidos, como foi dito anteriormente, é obtida através de técnicas de criptografia, onde se utiliza uma chave simétrica RC4 para criptografar os dados. Tanto o MN como o AP possuem uma mesma chave privada e uma chave pública compartilhada entre eles. Executa-se o algoritmo RC4 nas chaves pública e privada para se obter a Key-stream, e com essa última faz-se um XOR com os dados que serão enviados. As chaves compartilhadas possuem tamanho de 24 bits.

Confidentiality ou privacy



Garantia de privacidade com WEP utilizando RC4 [1]

Esquema da explicação do slide anterior e do posterior.

Integrity

- Cyclic Redundancy Check – CRC;
- CRC computado e associado ao Plaintext;
- CRC recalculado na máquina de destino;
- Não é um mecanismo seguro comparado a técnica Hash.

Como mostra a figura anterior, a integridade da mensagem é obtida através do CRC – Cyclic Redundancy Check. Calcula-se o CRC na mensagem original que posteriormente será associado a mesma para cifragem. No nó do destino, após a mensagem ser descifrada, é novamente recalculado o CRC para verificar a integridade da mensagem. O CRC não é um mecanismo seguro se comparado com a técnica Hash.

Utilização da mesma Key Stream

- Shared key de 24 bits;
  - Inevitável a reutilização da Key Stream.
  - Maior vulnerabilidade do protocolo!
- Dois campos utilizados pelo algoritmo RC4:
  - Secret key:
    - Uma chave constante.
  - Shared key:
    - Possibilidade de reutilização.
- XOR ed em pacotes com a mesma Key Stream:
  - Resultado XOR dos pacotes originais.
- Airsnort.

Uma das maiores vulnerabilidades do protocolo WEP é o tamanho de sua chave compartilhada de 24 bits. Isso faz com que acabe por reutilizar a mesma key stream. Como a key stream é obtida através dos dois campos que são utilizados pelo RC4, a secret key e a shared key. A primeira é uma chave constante, normalmente atribuída na configuração inicial de uma LAN e muitas vezes apenas alterada apenas quando essa configuração muda. Já a segunda é gerada aleatoriamente, porém com a limitação do comprimento, pode ser gerada a mesma. Caso se consiga obter dois pacotes cifrados com a mesma key stream, basta aplicar XOR ed nesses pacotes para eliminar a key stream, obtendo como resultado o XOR dos dois pacotes originais. Analisando-se a semelhança entre os bit streams dos dois pacotes, pode-se chegar a chave secreta, na maioria das vezes não diretamente, mas através de dicas.

Solução para vulnerabilidade na reutilização da Key Stream

- Aumento da Secret Key de 40 para 104;
  - Tornou maior o tempo de quebra;
  - Aumento da coleta de Interesting Packets.
- Solução proposta pela WiFi Alliance:
  - WiFi Protected Access – WPA.
- Solução do WPA:
  - Aumento da Shared key de 24 bits para 48 bits:
    - 16.7 milhões para 281 trilhões de possibilidades.
  - Dinamismo da Secret Key:
    - Mudança entre 10s-100s ou depois de um número de pacotes transmitidos;
    - Mudança realizada através do TKIP.

Como tentativa de solucionar essa vulnerabilidade do protocolo WEP, aumentarão a secret key de 40 para 104, porém o problema ainda não foi solucionado. Conseguiram apenas aumentar o tempo para se conseguir a quebra, como também o número de pacotes que seriam coletados. A WiFi Alliance propõe uma nova solução para o problema da vulnerabilidade do protocolo WEP, o WPA – WiFi Protected Access. Nessa solução propõe-se o aumento da shared key de 24 para 48 bits, aumentando de 16.7 milhões para 281 trilhões de possibilidades. A secret key deixa de constante e passa a possuir dinamismo, podendo haver mudança de acordo com o tempo ou pelo número de pacotes transmitidos.