SEGURANÇA EM REDES WI-FI: CONFIANDO MAIS, TRABALHANDO MELHOR

Everaldo Souto Salvador
Coordenação do Curso de Redes de Acesso em Telecomunicações – CEFET-PB
Av. 1º de Maio, 720 Jaguaribe CEP 58.015-430 João Pessoa - PB
E-mail: soutopb@yahoo.com.br

Tiago Ferreira Santos
Coordenação do Curso de Redes de Acesso em Telecomunicações – CEFET-PB
Av. 1º de Maio, 720 Jaguaribe CEP 58.015-430 João Pessoa - PB
E-mail: tiagoferreira_22@yahoo.com.br

Bruno Moreira da Silva
Coordenação do Curso de Redes de Acesso em Telecomunicações – CEFET-PB
Av. 1º de Maio, 720 Jaguaribe CEP 58.015-430 João Pessoa - PB
E-mail: moreirabbsilva@yahoo.com.br

RESUMO

As redes sem fio, wireless, englobam um conjunto de tecnologias – rádio freqüência, microondas, infravermelho, laser – aonde as diferenças vão desde a freqüência utilizada, as distâncias alcançadas, até os protocolos envolvidos – porém, incontestavelmente, a rede Wi-Fi, que é o padrão de internet sem fio, é a de maior notoriedade. Mas quais mecanismos nas redes Wi-Fi proporcionam uma adequada segurança ao seu usuário? Esta investigação tem como objetivo identificar soluções para sua implementação, observando suas características, analisando os riscos e possibilidades de utilização mais segura das redes Wi-Fi. Será feito um estudo exploratório, abordando desde a sua criação, seus estágios de desenvolvimento e ao padrão de segurança mais confiável da rede atualmente, o WPA2.

PALAVRAS-CHAVE: Wi-Fi, implementação, otimização, confiabilidade.

1. INTRODUÇÃO

Existe uma grande quantidade de tecnologias englobadas às redes sem fio, comumente conhecidas como redes wireless, que surgiram com o intuito de facilitar o acesso à internet nas áreas mais distantes dos grandes centros e de difícil acesso, pois estas demandam um alto custo para a instalação e manutenção da fibra óptica, material utilizado por uma rede cabeada, que é o meio mais comum de acesso à rede mundial de computadores. Estas tecnologias – rádio freqüência, microondas, infravermelho e laser são alguns exemplos – utilizam freqüências e protocolos diferentes e variam quanto ao alcance.

Comercialmente mais difundida, a rede Wi-Fi possui padrões que utilizam protocolos de segurança e autenticação de dados variados, uns mais eficazes que outros. Isso traz a tona uma discussão muito interessante, que é a respeito da segurança da rede Wi-Fi, tida por muitos com o calcanhar de Aquiles desta tecnologia.

Este projeto aborda desde o surgimento desta tecnologia e sua evolução até os dias atuais. Porém, seu principal objetivo é discutir e propor formas mais confiáveis de acesso à internet por meio da rede Wi-Fi, mostrando as vantagens e desvantagens dos principais protocolos de segurança, desde o WEP (Wired Equivalent Privacy ou protocolo para equivalência em fio) até o WPA2 (Wi-Fi Protected Access 2 ou proteção de acesso ao Wi-Fi, em português).

2. SISTEMAS WIRELESS

2.1 Origem

Os pioneiros no uso de redes sem fio foram os radioficcionados mediante suas emissoras, que oferecem uma velocidade de 9600 bps. Mas se falamos especificamente de redes sem fio, devemos voltar ao ano de 1997, no qual o organismo regulador IEEE (Institute of Electrical and Electronic Engineers - Instituto dos Engenheiros Elétricos e Eletrônicos) publicava 802,11 (802 faz referência ao grupo de documentos que descrevem as características das LANs ou Ethernet) dedicado a redes LAN sem fio. Dentro deste mesmo campo e anteriormente, no ano de 1995, temos o surgimento do Bluetooth, uma tecnologia da empresa Ericson, dedicada a conectar, mediante ondas de radio, os telefones moveis a diversos acessórios. Há pouco tempo, surgiu um grupo de estudo formado por fabricantes que estavam interessados nesta tecnologia para aplicá-la a outros dispositivos, como PDAs, terminais móveis ou inclusive eletrodomésticos.

Mas o verdadeiro desenvolvimento deste tipo de rede surgiu a partir do momento em que o FCC (Federal Communications Commission ou comissão federal de comunicação), organismo americano que é o equivalente ao que a ANATEL é no Brasil e que é encarregado de regular as emissões radioelétricas, aprovou o uso civil da tecnologia de transmissões de espectro disperso (SS ou spread spectrum, em inglês) embora a princípio tenha proibido o uso amplo desse espectro. Tal tecnologia já era utilizada no âmbito militar desde a segunda Guerra Mundial devido a suas extraordinárias características no que tange a dificuldade de sua detecção e tolerância a interferências externas.

As redes sem fio fornecem uma série de vantagens sobre as redes convencionais, já que não estão limitadas pelo uso de cabos, o que lhes concede uma maior mobilidade e liberdade de localização. Isto as torna sérias concorrentes das redes convencionais em locais onde e necessário uma grande mobilidade dos terminais, como no caso das fabricas, áreas de armazenagem do setor de embalagem, congressos ou escritórios temporários, nos quais a montagem de redes cabeadas, além de demandar a montagem uma infra-estrutura fixa, restringe a mobilidade dos terminais, que e uma condição imprescindível.

Um outro fato que pode ser observado é que as tecnologias de redes wireless atuais apontam para um objetivo comum: a implantação de inúmeras redes de comunicação, tantas quanto forem necessárias, para criar uma rede de âmbito mundial e proporcionar a inclusão total das pessoas, em todos os lugares, no ciberespaço (a tão falada inclusão digital). Essa tendência é apontada por diversos pesquisadores que prevêem ainda que, em um futuro bem próximo, onde quer que um indivíduo esteja ele estará coberto por uma rede, seja ela individual doméstica ou coletiva, com acesso à Internet vinte e quatro horas por dia, sete dias por semana.

2.2. Conceitos e Evoluções

As tecnologias de comunicação wireless seguem os padrões técnicos internacionais estabelecidos pelo IEEE (Institute of Electrical and Electronics Engineers), que definiu as especificações para a interconexão de equipamentos (computadores, impressoras, etc) e demais aplicações através do conceito "over-the-air", ou seja, proporciona o estabelecimento de redes e comunicações entre um aparelho cliente e uma estação ou ponto de acesso, através do uso de

freqüências de rádio. No padrão IEEE 802.11, é especificada a forma de ligação física e de enlace de redes locais sem fio, com o objetivo de fornecer uma alternativa às atuais conexões utilizando cabos.

Os padrões que recebem mais atenção ultimamente correspondem à família de especificações batizada de 802.11, conhecidas como Wireless Local Area Networks (WLAN's). A família de padrões IEEE 802.11 foi apelidada de Wi-Fi, abreviatura de Wireless Fidelity (fidelidade sem fios) marca registrada pertencente à WECA (Wireless Ethernet Compatibility Alliance), uma organização sem fins lucrativos criada em 1999 para garantir os padrões de interoperabilidade dos produtos Wi-Fi.

As redes sem fio (wireless) surgiram nos últimos anos em complemento e até mesmo em competição com o mundo das redes com fio (wireline). Assim, elas dão novo alcance às redes locais do tipo Local Area Network (LAN), nas chamadas Wireless Local Area Networks (WLANs). O mesmo se dá com a rede metropolitana (MAN, ou Metropolitan Area Network) e outras de cobertura nacional.

Os especialistas estimam que o mercado das redes locais sem fio vai explodir nos próximos meses, não apenas na América Latina, mas em todo o mundo. Essa é a opinião de Gil Simões, diretor comercial da Nortel Networks para a América Latina e o Caribe. Para ele, a demanda por acesso irrestrito, aliada a real necessidade de conectividade de banda larga, na região, conduzirá ao crescimento da alternativa rede local sem fio. Para isso contribuirá, também, a relativa ausência de produtos com tecnologia da linha de assinante digital (como ADSL).

Simões aponta o roaming de rede com muito melhores padrões de segurança como o ponto forte da nova solução Wi-Fi. Embora essas redes venham enfrentando problemas de segurança por muito tempo, Simões afirma que já se pode dar ao Wi-Fi um nível de segurança equivalente ao de uma rede fixa tradicional, como uma rede privada virtual IP (VPN-IP).

2.3 Caracterização

As redes wireless se caracterizam por:

- Maior produtividade - proporciona acesso "liberado" à rede em todo o campus e à Internet alem de oferecer a liberdade de deslocamento mantendo-se a conexão.
- Configuração rápida e simples da rede - sem cabos a serem instalados.
- Flexibilidade de instalação - podem ser instaladas em locais impossíveis para cabos e facilitam configurações temporárias e remanejamentos.
- Redução do custo de propriedade - as LANS sem fio reduzem os custos de instalação porque dispensam cabeamento; por isso, a economia é ainda maior em ambientes sujeitos a mudança freqüentes.
- Crescimento progressivo - as expansões e a reconfiguração não apresentam complicações e, para incluir usuários, basta instalar o adaptador de LAN sem fio no dispositivo cliente.
- Interoperabilidade - os clientes podem ficar tranqüilos com a garantia de que outras marcas de produtos compatíveis de rede e cliente funcionarão com as soluções propostas.

3. AS REDES WI-FI

As redes wi-fi não requerem cabos para transmitirem sinais; elas utilizam ondas de rádio ou infravermelho. Os sinais de radiofreqüência (RF) e de infravermelho são os mais utilizados para transmissão sem fio. A maioria das redes WLAN utiliza tecnologia de espectro distribuído. Sua largura de banda é limitada (geralmente inferior a 11Mpbs) e os usuários compartilham a largura de banda com outros dispositivos do espectro.

3.1 O Surgimento das Redes Wi-Fi

Wi-Fi é o nome da marca comercial utilizada pela WECA (Wireless Ethernet Compatibility Alliance) para indicar a interoperabilidade de produtos WLAN. O nome provém de "wireless fidelity" (fidelidade sem fio). A WECA submete os produtos WLAN a testes avançados; os produtos que atendem ao padrão de interoperabilidade recebem o logotipo Wi-Fi.

3.2 A Estrutura de uma Rede Wi-Fi

A forma de conexão e de compartilhamento de uma rede wi-fi é estabelecida de acordo com a arquitetura adotada, sendo definidas três arquiteturas básicas:

- Redes ad hoc, ou IBSS (Independent Basic Service Set) - compostas por estações independentes, sendo criadas de maneira espontânea por estes dispositivos. Este tipo de rede se caracteriza pela topologia altamente variável, existência por um período de tempo determinado e baixa abrangência;
- Redes de infra-estrutura básica, ou BSS (Basic Service Set), são formadas por um conjunto de estações sem fio, controladas por um dispositivo coordenador denominado AP (Access Point). Todas as mensagens são enviadas ao AP que as repassa aos destinatários. O AP funciona com o mesmo princípio de um equipamento concentrador (hub) para o ambiente sem fio e operando como uma ponte (bridge) entre o ambiente sem fio e a rede fixa;
- Redes de infra-estrutura - também denominadas ESS (Extended Service Set). Estas redes são as uniões de diversas redes BSS conectadas através de outra rede (como uma rede Ethernet, por exemplo). A estrutura deste tipo de rede é composta por um conjunto de AP's interconectados, permitindo que um dispositivo migre entre dois pontos de acesso da rede. As estações vêem a rede como um elemento único.

Através da utilização de portadoras de rádio ou infravermelho, as redes wi-fi estabelecem a comunicação de dados entre os pontos da rede. Os dados são modulados na portadora de rádio e transmitidos através de ondas eletromagnéticas.

Múltiplas portadoras de rádio podem coexistir num mesmo meio, sem que uma interfira na outra. Para extrair os dados, o receptor sintoniza numa freqüência específica e rejeita as outras portadoras de freqüências diferentes.

Num ambiente típico, como o mostrado na Figura 1, o dispositivo transceptor (transmissor/receptor) ou ponto de acesso (*Access point*) é conectado a uma rede local Ethernet convencional (com fio). Os pontos de acesso não apenas fornecem a comunicação com a rede convencional, como também intermedeiam o tráfego com os pontos de acesso vizinhos, num esquema de micro células com *roaming* semelhante a um sistema de telefonia celular.

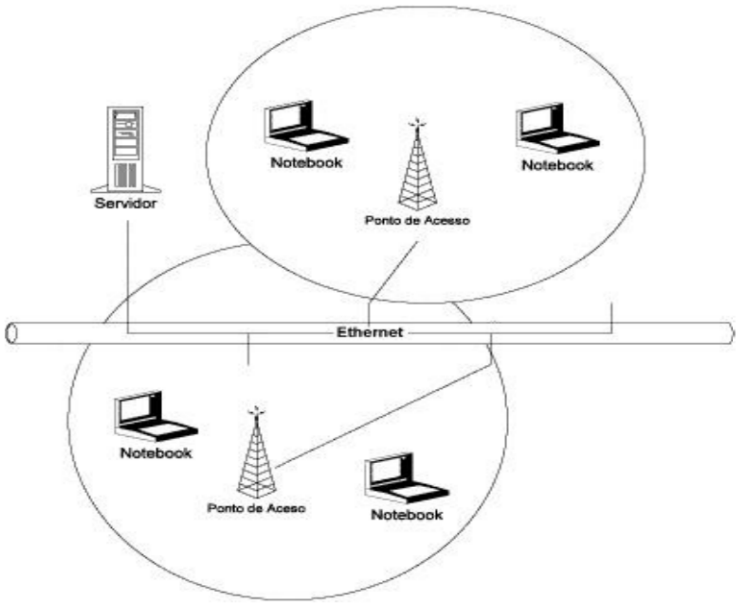


Figura 1 - Rede Wireless LAN típica

3.3 Os Principais Padrões de Redes Wi-Fi, Suas Especificações e Evoluções

Na família de padrões de rede IEEE 802.11, designação das redes Wi-Fi, seguindo a ordem de surgimento no mercado, as principais especificações são: 802.11a, 802.11b, 802.11g, 802.11i e 802.11e.

O padrão 802.11a surge como o mais indicado para empresas que, dentro de um espaço reduzido, concentrem um alto número de usuários, pois oferece uma largura de banda de 54 Mbps (Megabits por segundo) e um raio de alcance de até 40 metros, operando na freqüência de 5 GHz, proporcionando uma comunicação menos vulnerável a interferências.

O padrão 802.11b oferece uma largura de banda de 11 Mbps, com um raio de alcance de até 120 metros, operando na freqüência de 2.4 GHz. Quando surgiu, tornou-se muito popular pelo baixo custo que representava sua adoção. Porém, o padrão 802.11g veio como uma evolução ao primeiro, pois, utilizando-se de uma tecnologia de modulação mais avançada, propicia uma largura de banda quase cinco vezes maior, de 54 Mbps. Isso trouxe uma melhora significativa para o sinal, dando maior velocidade e possibilitando modelos de segurança mais robustos, embora operando na mesma freqüência e oferecendo o mesmo alcance do 802.11b.

É interessante citar que alguns desses padrões não são compatíveis entre si. Por exemplo, o 802.11a e o 802.11b utilizam-se de freqüências diferentes, fazendo com que a placa de um padrão não funcione com um concentrador ou placa de outro. Analogamente, é como um rádio AM, que não sintoniza estações FM por não possuir recursos para tanto.

Atualmente, são fabricadas placas de rede que suportam padrões como o 802.11a, 802.11b e 802.11g simultaneamente, o que torna a mobilidade fácil para o usuário.

O padrão 802.11i foi quem trouxe o WPA2, a solução em segurança para redes wi-fi e que será abordado adiante neste artigo.

O mais recente padrão de redes wi-fi, o 802.11e trouxe o QoS (Quality of Service ou qualidade de serviço), que há muito as redes wi-fi almejavam e hoje é uma realidade.

4. A SEGURANÇA DAS REDES WI-FI

4.2 A Necessidade de uma Rede Mais Segura

Devido ao alto índice de invasões em redes Wi-Fi, tornou-se necessária a busca por modelos que proporcionassem maior confiabilidade a esta rede. Era arriscado enviar dados confidenciais pela rede, já que o meio de transmissão por onde trafegam as informações é o ar, tornando a captura de informações um trabalho simples para quem possuísse um bom conhecimento acerca das tecnologias wireless. Criou-se, então, a criptografia de dados, para que estes pudessem ser enviados e trafegados de forma segura pelo ar.

4.3 As Falhas na Segurança

Existem duas vulnerabilidades em redes Wi-Fi, que são: a forma como é instalado e configurado o padrão da rede, e a criptografia utilizada para proteger as informações. Não adianta ter o melhor padrão de segurança existente no mercado mal instalado ou configurado incorretamente. Com pouco tempo, descobriu-se também um modo de "quebrar" a criptografia dos dados da rede Wi-Fi.

Os protocolos de WLAN existentes utilizavam WEP (Wired Equivalent Privacy, algo como protocolo para equivalência em fio), recurso de segurança empregado para assegurar a autenticação, integridade e confidencialidade da conexão.

No que diz respeito à autenticação, o WEP lança mão do conceito de chave compartilhada, que se baseia no algoritmo de criptografia RC4 (Rivest Cipher 4), um dos algoritmos de encriptação de fluxo mais utilizados, podendo empregar chaves de criptografia de 64 a 256 bits. Porém o RC4 possui falhas em sua arquitetura e, capturando um grande numero de pacotes, o que leva várias horas, é possível quebrar ou descobrir a chave de criptografia do WEP usando ferramentas de diversos tipos e encontradas gratuitamente na internet.

Criou-se então o WPA (Wi-Fi Protected Access ou acesso protegido wi-fi), a fim de corrigir algumas vulnerabilidades existentes no WEP que facilitavam sua quebra. Utilizando o protocolo de chave temporária TKIP (Temporal Key Integrity Protocol), que possibilita a criação de chaves por pacotes, houve uma melhora substancial na criptografia de dados. O TKIP tem como principal característica a mudança freqüente de chaves, que se alteram a cada novo envio de pacote, o que garante mais segurança a rede. Possui um mecanismo de distribuição de chaves além de uma função detectora de erros, um vetor de inicialização de 48 bits, ao invés dos 24 bits desta função no WEP.

O WAP também melhorou o processo de autenticação dos usuários, que utiliza o EAP (Extensive Authentication Protocol ou protocolo de autenticação extensivo), que faz a autenticação de cada usuário antes de acessar a rede através de um servidor de autenticação central. O dinamismo da chave de criptografia do WPA é uma das grandes diferenças em relação ao WEP, que utilizava uma mesma chave repetidamente e onde as trocas de chaves eram feitas manualmente, o que, convenientemente, não é necessário no WPA. Sem dúvidas, o WPA foi uma evolução

bem sucedida em relação ao WEP, tornando a rede muito mais segura. Porém, essa evolução não foi perfeita e, capturando pacotes com TKIP, o que é difícil, é possível descobrir e quebrar a chave de criptografia do WPA.

4.4 WPA2: A Atual Solução Para a Segurança das Redes Wi-Fi

O WPA2 (Wi-Fi Protected Access 2) é o mais recente e seguro padrão de segurança para redes Wi-Fi, pois até o momento não foi detectado falhas que possibilitem a quebra de sua chave de segurança. O WPA2 também trabalha com o conceito de chave temporal, que já existia no WPA. Porém, além de suportar chaves de segurança de até 256 bits, este padrão troca a chave de segurança a cada 10 k de dados emitidos pela rede, tornando sua criptografia dificílima de ser decifrada e violada a tempo.

O WPA2 utiliza o algoritmo CBC-MAC (Counter Mode Cipher Block Chaining-Message Authentication Code, algo como código de autenticação de mensagem encadeada em modo contador de cifras em bloco), também conhecido como CCMP, que é um modo específico do AES (Advanced Encryption Standard ou padrão de criptografia avançada), e que foi criado para fornecer uma integridade de dados muito mais forte e fazendo o rechaveamento automaticamente para derivar novos conjuntos de chaves temporais. Esses conjuntos de chaves temporais derivam de uma chave mestra e de outros valores. Em resumo, o CBC-MAC oferece confidencialidade, autenticação da origem e integridade dos dados de quadros sem fio 802.11.

4.5 Processo de Criptografia e Descriptografia do WPA2

De acordo com o artigo The Cable Guy (2005), O CCMP do AES usa o CBC-MAC para calcular o MIC e o modo de contador do AES para criptografar a carga do 802.11 e o MIC.

O algoritmo CBC-MAC calcula um valor de 128 bits, e o WPA2 usa os 64 bits de ordem superior como um MIC (Message Integrity Code ou código de integridade da mensagem), que é calculado da seguinte forma:

1. Criptografa um bloco inicial de 128 bits com o AES e a chave de integridade de dados. Isso produz um resultado de 128 bits (Resultado1).
2. Executa uma operação OR (XOR) exclusiva entre Resultado1 e os 128 bits de dados seguintes pelos quais o MIC está sendo calculado. Isso produz um resultado de 128 bits (XResultado1).
3. Criptografa o XResultado1 com o AES e a chave de integridade de dados. Isso produz o Resultado2.
4. Executa um XOR entre Resultado2 e os 128 bits de dados seguintes. Isso produz o XResultado2.

As etapas 3-4 se repetem para os blocos de 128 bits adicionais dos dados. Os 64 bits de ordem superior do resultado final são o MIC do WPA2. A figura2 mostra o processo de cálculo do MIC.

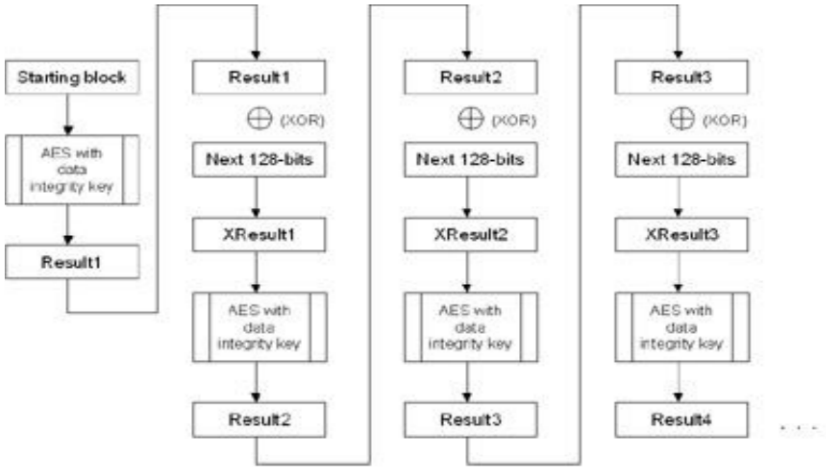
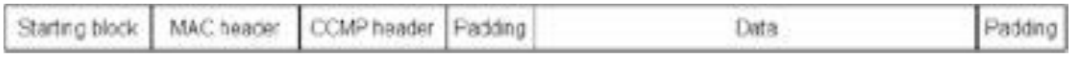


Figura 2 – Processo de cálculo do MIC

Para calcular o MIC de um quadro IEEE 802.11, o WPA2 constrói o seguinte:



- O bloco inicial é um bloco de 128 bits descrito posteriormente neste artigo.
- O cabeçalho MAC é o cabeçalho MAC 802.11 com os valores dos campos que podem ser alterados em trânsito definidos como 0.
- O cabeçalho CCMP tem 8 bytes e contém o campo Número do pacote de 48 bits e campos adicionais.
- Os bytes de preenchimento (definidos como 0) são adicionados para garantir que a parte do bloco de dados inteiro até os dados de texto sem formatação seja um número integral de blocos de 128 bits.
- Os dados são a parte de texto sem formatação (não criptografados) da carga do 802.11.
- Os bytes de preenchimento (definidos como 0) são adicionados para garantir que a parte do bloco de dados do MIC que inclui os dados de texto sem formatação seja um número integral de blocos de 128 bits.

O WPA2 criptografa o MIC com a criptografia do modo de contador do AES, que utiliza o seguinte processo:

1. O algoritmo de criptografia do modo de contador do AES Criptografa um contador inicial de 128 bits com o AES e a chave de criptografia de dados. Isso produz um resultado de 128 bits (Resultado1).
2. Executa uma operação OR (XOR) exclusiva entre Resultado1 e o primeiro bloco de 128 bits dos dados que estão sendo criptografados. Isso produz o primeiro bloco criptografado de 128 bits.
3. Incrementa o contador e o criptografa com o AES e a chave de criptografia de dados. Isso produz o Resultado2.
4. Executa um XOR entre Resultado2 e os 128 bits de dados seguintes. Isso produz o segundo bloco criptografado de 128 bits.

O modo de contador do AES repete as etapas 3-4 para os blocos de 128 bits adicionais de dados, até o bloco final. Para o bloco final, o modo de contador do AES executa o XOR do contador criptografado com os bits restantes, produzindo dados criptografados do mesmo comprimento que o último bloco de dados. A figura 3 mostra o processo do modo de contador do AES.

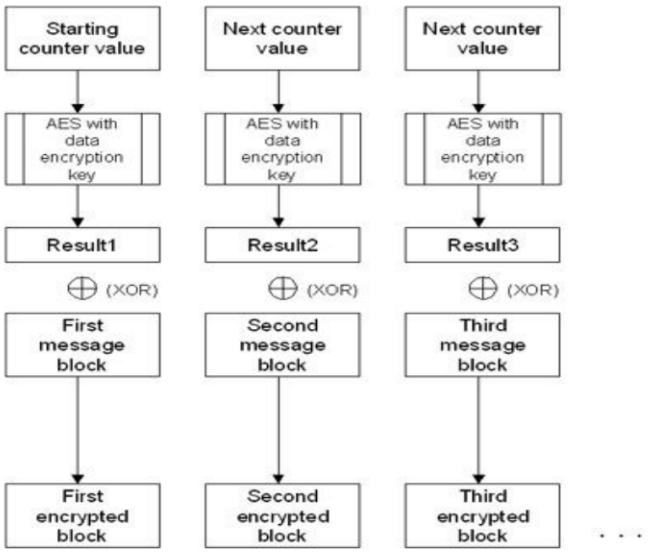


Figura 3 – Processo do modo de contador do AES

Para criptografar um quadro de dados em unicast, o WPA2 usa o seguinte processo:

1. Insere o bloco inicial, o cabeçalho MAC 802.11, o cabeçalho CCMP, o comprimento dos dados e campos de preenchimento no algoritmo CBC-MAC com a chave de integridade de dados para produzir o MIC.
2. Insere o valor do contador inicial e da combinação dos dados com o MIC calculado no algoritmo de criptografia do modo de contador do AES com a chave de criptografia de dados para produzir os dados criptografados e o MIC.
3. Adiciona o cabeçalho CCMP contendo o Número do pacote à parte criptografada da carga do 802.11 e encapsula o resultado com o cabeçalho e as informações finais do 802.11. A figura 4 mostra o processo de criptografia do WPA2 para um quadro de dados em unicast.

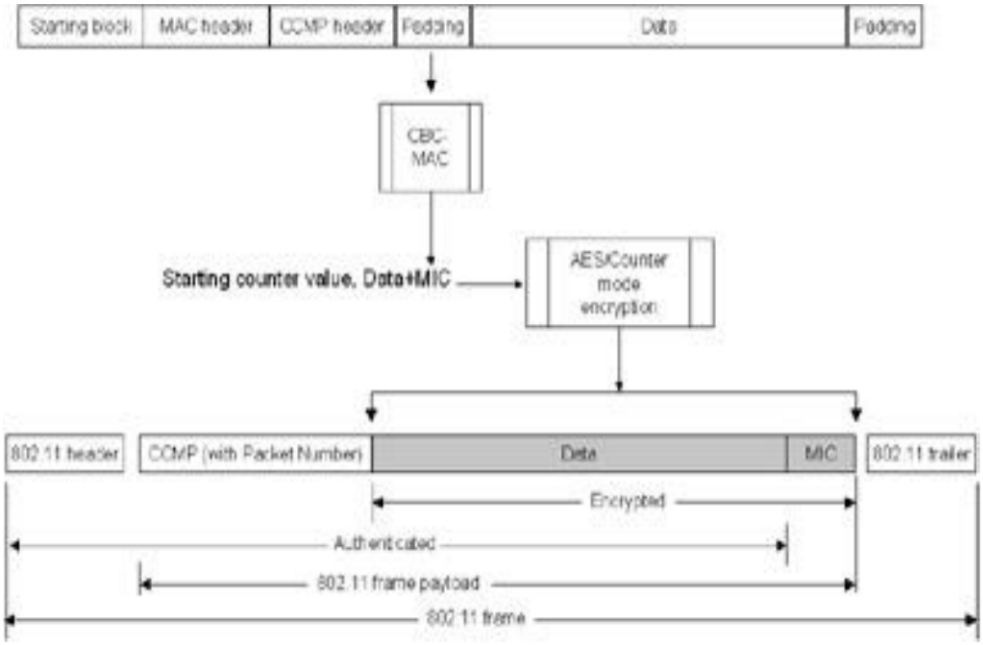


Figura 4 – Processo de criptografia do WPA2 em um quadro de dados unicast

Para descriptografar um quadro de dados em unicast e verificar a integridade dos dados, o WPA2 usa o seguinte processo:

1. Determina o valor do contador inicial a partir dos valores nos cabeçalhos do 802.11 e do CCMP.
2. Insere o valor do contador inicial e a parte criptografada da carga do 802.11 no algoritmo de descriptografia do modo de contador do AES com a chave de criptografia de dados para produzir os dados descriptografados e o MIC. Para a descriptografia, o modo de contador do AES executa o XOR do valor do contador criptografado com o bloco de dados criptografados, produzindo o bloco de dados descriptografados.
3. Insere o bloco inicial, o cabeçalho MAC 802.11, o cabeçalho CCMP, o comprimento dos dados e campos de preenchimento no algoritmo CBC-MAC do AES com a chave de integridade de dados para calcular o MIC.
4. Compara o valor calculado do MIC com o valor do MIC não criptografado. Se os valores do MIC não corresponderem, o WPA2 descartará os dados silenciosamente. Se os valores do MIC corresponderem, o WPA2 passará os dados para as camadas de rede superiores para processamento. A figura 5 mostra o processo de descriptografia do WPA2 para um quadro de dados em unicast.

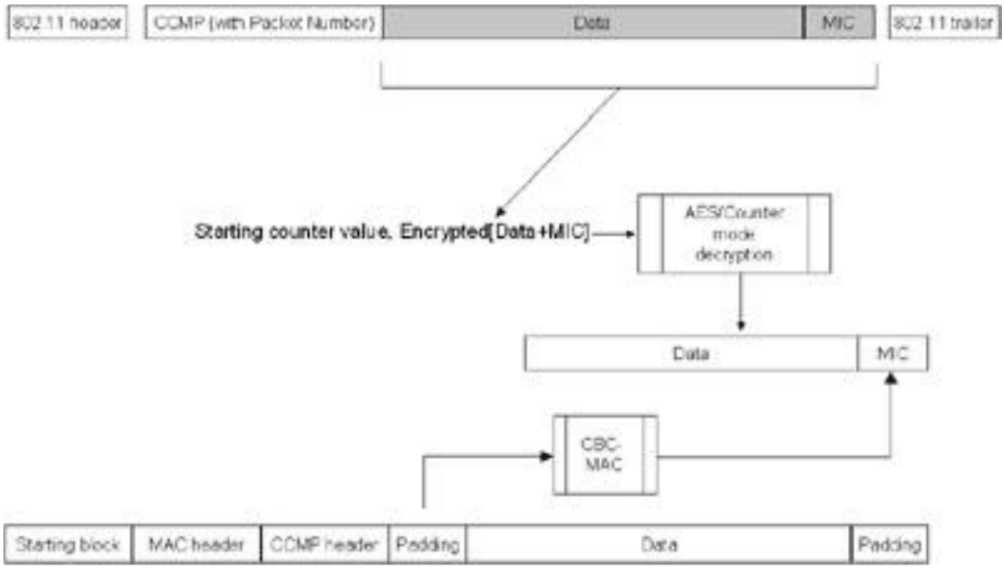


Figura 5 – Processo de descriptografia do WPA2 para quadro de dados unicast

O ponto forte do WPA2 é que não foram registrados, até o momento, ataques com êxito a sua segurança, pois as técnicas utilizadas para burlar os outros padrões são ineficazes neste. Somente foram registrados side-channel attacks, que são falhas físicas. Isso torna o WPA2 a melhor solução no que diz respeito à segurança em redes sem fio, atualmente. Um possível ponto fraco desse padrão, se é que se pode dizer que se trata de um ponto fraco, é que por conta de sua avançada criptografia, podem ser necessários novos Hardwares para suportar o WPA2.

5. CONSIDERAÇÕES FINAIS

Não existe garantia de segurança exclusivamente por meios técnicos. Quem assim o faz não conhece o problema, tampouco a tecnologia, pois a segurança não é uma questão meramente tecnológica, também trata-se de procedimentos adotados, como trocar as senhas pré-determinadas dos pontos de acesso, ativar a filtragem de endereços MAC, limitar o número de equipamentos que possam acessar a rede simultaneamente, ativar firewall, modificar o SSID de forma pré-definida e ocultá-lo, por exemplo.

Não adianta ter o melhor padrão de segurança, adotar várias medidas de proteção se não houver uma boa instalação e configuração destes mecanismos. Quanto maior a dificuldade, menor é o interesse em burlar a segurança de uma rede, pois quem vê várias medidas como esta, está ciente de que quem projetou a rede tem um bom conhecimento de segurança.

6. REFERÊNCIAS BIBLIOGRÁFICAS

http://www.microsoft.com/technet/community/columns/cableguy/cg0505.mspx
http://www.mobilelife.com.br
http://www.secforum.com.br/categories.php?op=newindex&catid=5
http://pt.wikipedia.org
http://www.wirelessbrasil.org/