Segurança

Fernando Verissimo
verissimo@ravel.ufrj.br http://www.ravel.ufrj.br/~verissimo

Orientação : Prof. Luis Felipe M. de Moraes
moraes@cos.ufrj.br http://www.cos.ufrj.br/~moraes

Apresentação para o GARF
Grupo de Atuação em Redes sem Fio

Referências Bibliográficas

1. Barbosa, A.S. and De Moraes, L.F.M. Curso de Sistemas de Segurança de Informação.
2. Borisov, N., Goldberg, I. And Wagner, D. 2001. Intercepting Mobile Communications: The Insecurity of 802.11. The Seventh Annual International Conference on Mobile Computing and Networking. July 16-21, 2001, Rome, Italy.
3. Campello, R.S. and Weber, R. 2001. Minicurso de Sistemas de Detecção de Intruso. In: 19º Simpósio Brasileiro de Redes de Computadores. Florianópolis, 21 a 25 de maio de 2001.
4. De Carvalho, D.B. 2000. Segurança de Dados com Criptografia: Métodos e Algoritmos. Rio de Janeiro:Book Express;
5. Ellison, C. 2001. Exploiting and Protecting 802.11b Wireless Networks. In: ExtremeTech. Sep. 4, 2001;
6. Fluhrer, S., Mantin, I. And Shamir, A. 2001. Weakness in the Key Scheduling Algorithm of RC4. Presented at 8th Annual Workshop on Selected Areas in Cryptography. 23pp;

Referências Bibliográficas

7. Mariano, I. Da S. 2000. IPSec e DDos, Aspectos de Segurança em Redes TCP/IP. Seminário de Tópicos Especiais em Redes Integradas Faixa Larga. COPPE/Sistemas.
8. Meredith, G. 2001. Securing the Wireless LAN. Packet magazine. vol 13. no 3. Pp 74-77.
9. Negus, K.J., Stephens, A.P. and Lansford, J. HomeRF: Wireless Networking for the Connected Home. http://www.homerf.org
10. Orman, H. K. The OAKLEY Key Determination Protocol. http://www.imib.med.tu-dresden.de/imib/Internet/Literatur/ISAKMP/draft-ietf-ipsec-oakley-02.txt. Last Access: 06-Dec-01.
11. Paulson, L.D. 2000. Exploring the Wireless LANscape. Computer Magazine, Outubro/2000
12. Shannon, C.E. 1948. A Mathematical Theory of Communication. The Bell System Technical Journal. Vo.27,pp.379-423, 623-656,Julho,Outubro de 1948.

Referências Bibliográficas

13. Soares, L.F.G., Lemos, G. and Colcher, S. 1995. Redes de Computadores: das LANs, MANs e WANs às redes ATM. Rio de Janeiro: Campus.
14. Stallings, W. 1998. Cryptography and Network Security. 2nd ed. New Jersey: Prantice-Hall. pp. 190-193;399-440;
15. Stubblefield, A., Ioannidis, J. and Rubin, A.D. 2001. Using the Fluhrer, Mantin, and Shamir Attack to Break WEP. ATT&T Labs Technical Report TD-4ZCPZZ. Rev. 2. Aug. 21, 2001;
16. Tanembaum, A.S. 1944. Redes de Computadores. 1997.Tradução da Terceira Edição. Rio de Janeiro:Campus.
17. Terada, R. 2000. Segurança de Dados: Criptografia em Redes de Computadores. São Paulo:Edgard Blücher.

Criptografia

- Criptografia
  - Surgiu da necessidade de se enviar informações sensíveis através de meios de comunicação não confiáveis.
  - A forma de contornar esse problema é utilizar um método que modifique o texto original através de um processo de codificação definido por um método de criptografia.

Criptografia

- É a idéia de “esconder” ou “camuflar” informações sigilosas de qualquer pessoa desautorizadas a lê-las, isto é, de qualquer pessoa que não conheça a chave secreta de criptografia

Criptografia

Criptografia

- Como foi apresentado na figura anterior, bastaria ao hacker ou o cracker descobrir o método de criptografia e ele poderia acessar todas as informações.
- Um novo método de criptografia teria que ser construído.

Criptografia

- Chaves
  - No método de criptografia com chaves, a saída do procedimento: O texto criptografado, não é mais só função do texto normal, mas função da chave de codificação também.
  - Existe uma chave de codificação e outra, que pode ser distinta ou não, chamada chave de decodificação.
    - Criptografia simétrica
    - Criptografia assimétrica

Criptografia: Cifra de Cæsar

- FERNANDO=MLYUHUKV

A	B	C	D	E	F	G	H	I	J	K	L	M
H	I	J	K	L	M	N	O	P	Q	R	S	T

N	O	P	Q	R	S	T	U	V	W	X	Y	Z
U	V	W	X	Y	Z	A	B	C	D	E	F	G

- Chave=19 --- Total de chaves=25

Criptografia

- Até o fim da década de 70, todos os algoritmos eram secretos.
- Hoje em dia, os algoritmos são abertos e , publicados, principalmente nas reuniões técnicas (CRYPTO, nos EUA, e a EUROCRYPT)
- Até hoje não se conhece um método matemático para provar que o algoritmo é seguro.

Criptografia: Substituição Simples

- Substituição simples

A	B	C	D	E	F	G	H	I	J	K	L	M
I	N	K	R	F	S	M	W	A	X	J	P	Z

N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Q	G	T	Y	B	D	E	O	H	V	L	U	C

- FERNANDO=SFBQIQRG
- 25! chaves

Criptografia

- Cifra de Vigenère

1	2	3	4	5	6	7	8
F	E	R	N	A	N	D	O
5	4	17	13	0	13	3	14
C	O	N	A	C	O	N	A
2	14	13	0	2	14	13	0
5+2	4+14	17+13	13+0	0+2	13+14	3+13	14+0
7	18	5	13	2	1	16	14
H	S	F	N	C	B	Q	O

- Chave: CONA
- Total de chaves=26^n, onde n é o tamanho da chave
- Cifra de Vigenère-Vernam – Chave não repete, do mesmo tam.

Criptografia

- Transposição – n = 4

1	2	3	4	1	2	3	4
F	E	R	N	A	N	D	O
3	1	4	2	3	1	4	2
R	F	N	E	D	A	O	N

- Chave: (3, 1, 4, 2)
- Total de chaves = n!-1

Algoritmo Criptográfico

- Composição
  - A maioria dos algoritmos modernos consiste em compor várias funções, de forma que o resultado de uma seja o parâmetro da próxima.

Algoritmo Criptográfico

- DES – Data Encryption Standard
  - Desenvolvido pela IBM e adotado pelo governo americano.
  - Codifica blocos de 64 bits.
  - O algoritmo de codificação parametrizado por chave de 56 bits e possui estágios diferentes.
  - Um dos principais problemas desse método e dos algoritmos de criptografia simétricos é a exigência que o transmissor e o receptor de uma mensagem conheçam a única chave secreta usada na codificação e na decodificação.

Algoritmo Criptográfico

- RSA (Rivest-Shamir-Adleman)
  - Método de criptografia assimétrico
  - Baseia-se na dificuldade de se fatorar números grandes.
  - Segundo os autores do método na sua publicação "*On a Method for Obtaining Digital Signatures and Public Key Cryptosystems*" a fatoração de um número de 200 dígitos leva aproximadamente 4 bilhões de anos em tempo de computação.

WEP

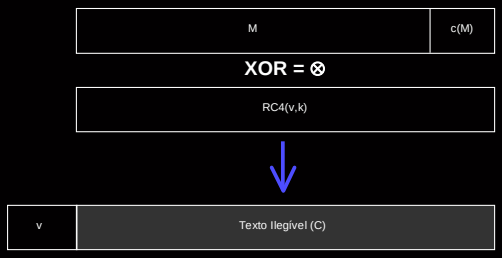
- Wired Equivalent Privacy
- Utiliza a mesma chave para codificar e decodificar
- Possui três objetivos principais:
  - Confidencialidade: Garantir que ninguém lerá a mensagem
  - Controle de Acesso: Garantir que só pacotes confiáveis trafegarão pelo sistema.
  - Integridade dos dados: Garantir que não haverá modificações na mensagem.

Algoritmo WEP

- M – Mensagem legível
- c(M) – Resultado da submissão de M à um algoritmo de checksum (CRC32), com intuito de garantir a integridade da mensagem
- P – <M,c(M)>

- Submissão de P à um algoritmo de geração de n° pseudo-aleatório (RC4), que recebe como parâmetro, a chave, k, e um vetor de inicialização, v

Algoritmo WEP



RC4 – Ron's Cipher 4

- Criado por Ron Rivest em 1987
- Pertence hoje à RSA Security
- É um algoritmo de fluxo
- Gera ilimitados bytes pseudo-aleatórios
- Tem chave de tamanho variado

RC4 – KSA (Key Scheduling Algorithm)

- RC4 recebe chave *ch* de n_{ch} bits (máx 2.048)
- Tem que gerar S de 256 bytes ($S=s_0,s_1,\ldots,s_{255}$)
- Algortimo:

1. Para i de 0 a 255 faz-se:
   a. $s_i \leftarrow i$
2. Seja o vetor de 256 bytes(2048 bits) $K=(k_0,k_1,\ldots,k_{255})$
3. Copia a ch para K, bit a bit, repetindo-se quantas vezes forem necessárias
4. $j \leftarrow 0$
5. Seja t um byte
6. Para I de 0 a 255 faz-se
   a. $j \leftarrow (j+s_i+k_i) \bmod 256$
   b. $t \leftarrow s_i$
   c. $s_i \leftarrow s_j$
   d. $s_j \leftarrow t$

Fonte: [DECAR]

- S é uma permuta dos números de 0 a 255

GARF

RC4 – PRGA (Pseudo-Random Generating Algorithm)

1. $i \leftarrow 0$
2. $j \leftarrow 0$
3. Seja t um byte
4. Enquanto forem necessários bytes b aleatórios faz-se:
   a. $i \leftarrow (i+1) \bmod 256$
   b. $j \leftarrow (j+s_i) \bmod 256$
   c. $t \leftarrow s_j$
   d. $s_i \leftarrow s_j$
   e. $s_j \leftarrow t$
   f. $t \leftarrow (s_i + s_j) \bmod 256$
   g. $b \leftarrow s_t$
   h. O byte aleatório será b

GARF

Análise da Fragilidade do Protocolo WEP

- O aumento da chave faz o uso da força bruta quase impossível.
- Risco da reutilização da chave composta

$$C_1 = P_1 \otimes RC4(v,k)$$
$$C_2 = P_2 \otimes RC4(v,k)$$

Relembrando propriedades do XOR

A	A	A⊗A
1	1	0
0	0	0

A	0	A⊗0
1	0	1
0	0	0

A	B	C	(A⊗B)⊗C	A⊗(B⊗C)
1	1	1	1	1
1	1	0	0	0
1	0	1	0	0
1	0	0	1	1
0	1	1	0	0
0	1	0	1	1
0	0	1	1	1
0	0	0	0	0

GARF

Análise da Fragilidade do Protocolo WEP

- k é constante em todos os pacotes
- O padrão WEP recomenda (não exige) que v varie para cada pacote
- O padrão não diz como gerar v, algumas implementações faz isso de forma pobre.
- v tem 24 bits de comprimento.
- Imagine uma implementação que envia pacotes de 1500 bytes à uma taxa média de 5Mbps (o máximo é 11Mbps) e a cada envio de pacotes ele incrementa o v retornando a zero após o último valor. Esse processo demorar menos de meio dia. Veja:

$$5Mbits/8*1500 \approx 416\,pac/s$$
$$2^{24}/416 \approx 40.329s \quad ou \quad 11h12m$$

- 50% de chances de colisão depois de 4823 pacotes

Análise da Fragilidade do Protocolo WEP

- Com o tempo o criptoanalista pode criar um dicionário de chaves compostas.
- Supondo um pacote de 1500 bytes com 2^{24} diferentes valores de v, o espaço necessário para montar o dicionário é de 24GB
- Esse dicionário não depende do valor de k, mas somente de v.

Análise da Fragilidade do Protocolo WEP

- Autenticação de mensagem: WEP usa o algoritmo de checksum para garantir a integridade.
- O algoritmo utilizado é o CRC-32, que é criptografado junto com a mensagem. Esse algoritmo é linear, ou seja,

$$C = RC4(v,k) \otimes \langle M, c(M) \rangle$$
$$M' = M \otimes \Delta$$
$$C = C \otimes \langle \Delta, c(\Delta) \rangle = RC4(v,k) \otimes \langle M, c(M) \rangle \otimes \langle \Delta, c(\Delta) \rangle =$$
$$= RC4(v,k) \otimes \langle M \otimes \Delta, c(M) \otimes c(\Delta) \rangle = RC4(v,k) \otimes \langle M', c(M) \otimes c(\Delta) \rangle =$$
$$RC4(v,k) \otimes \langle M', c(M') \rangle$$

- Tráfego novo também pode ser criado.

WEP2

– IV tem 128 bits

$$5Mbits/8*1500 \simeq 416\,pac/s$$
$$2^{128}/416 \simeq \infty$$

– CRC32 permanece

Segundo ataque ao WEP

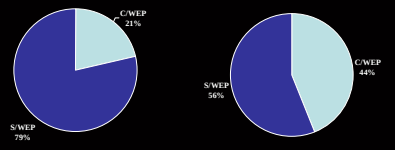
- Baseado no artigo "*Using the Fluhrer, Mantin, and Shamir Attack to Break WEP" de* Stubblefield et al
- Descobriram uma correlação muito forte no primeiro byte da cadeia pseudoaleatória do algoritmo RC4 com os bytes da chave;
- Também utilizaram o trabalho de Borisov, Goldberg e Wagner (Berkeley).

Novas comprovações da vulnerabilidade do WEP

- Craig Ellison, da Extremetech, Eric McIntyre, da TZO.com, Christopher Hose, da Stevens Tech University;
- Eles percorreram Manhatham com um Notebook, um cartão Wi-fi IEEE802.11b Orinoco-gold, uma antena, bisbilhotando as redes.
- Utilizaram o NetStumbler e o Airsnort

Resultados da pesquisa de campos

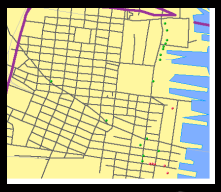
- Primeiro resultado mostrou que dos 61 pontos de acessos capturados pelo equipamento no quarteirão em que eles fizeram o primeiro teste, 48 deles não tinham o protocolo WEP habilitado.



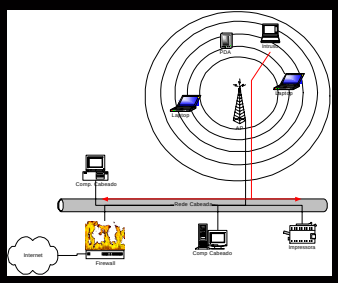
Manhathan e Silicon Valley

Resultados da pesquisa de campos

- Eles pegaram uma rede ao acaso;
- O DHCP dessa rede enviou um número IP;
- Na mesma rede eles apontaram o browser do notebook para o roteador, que estava com a senha default do roteador.
- Com o auxílio do GPS;



AP atrás do Firewall



Sugestões para a melhoria da segurança

- Habilitar o WEP. Todas as implementações vem utilizando tecnologia Wi-Fi;
- Altere o SSID dos produtos. Eles encontraram muitos roteadores com os SSID defaults, e por coinscidência, ou não, com as senhas defaults. E não altere para coisa que estejam relacionadas com o nome da empresa, o nome da rua, nome do produto principal da empresa;
- Desabilite a opção "broadcast SSID". Com o "broadcast SSID" habilitado, o ponto de acesso aceitará qualquer um SSID;
- *Evite colocar o ponto de acesso perto da janelas. Instale-o próximo ao centro do prédio;*
- Crie uma tabela de endereços MAC nos APs;

Sugestões para a melhoria da segurança

- Use um nível adicional de protocolo de autenticação (Ex.: RADIUS);
- Desligue o serviço de DHCP para os dispositivos wireless. Crie uma subrede diferente só para os dispositivos wireless;
- Não compre dispositivos de rede que só aceitem WEP de 64 bits;
- Somente compre APs que têm firmwares atualizáveis. Existe um grande número de melhorias sendo desenvolvidas e que você desejará atualizar no seu AP.

Em defesa de Rivest

- O artigo "Weaknesses in the Key Scheduling Algorithm of RC4" diz que o algoritmo de seleção da chave é muito simples;
- Ron Rivest responde que o que foi quebrado é o protocolo WEP, e que o algoritmo RC4, que está inserido em outros protocolos não é tão trivial;
- A RSA aconselha uso de um algoritmo de segurança em camadas mais altas e a troca do CRC por um algoritmo de espalhamento (*hash*), como por exemplo o MD5;
- A WECA (Wireless Ethernet compatibility Alliance) diz já ter predito que uma camada de segurança end-to-end deveria ser instalada, mesmo se o WEP não tivesse sido comprometido.

Passando a régua

- RC4 é seguro ? Porque o WEP insiste com o RC4 e não coloca um algoritmo mais seguro, como, por exemplo o RC5 e MD5 (ou SHS) ?
- WEP pode ser mais seguro ? Soluções CISCO
- Estudar VPN
- Caminho do IEEE
  - FPK [RSA] – Fast Packet Keying
  - TKIP [WECA] – Temporary Key Integrity Protocol
  - NIST/USA quer AES (Advanced Encryption Standard)