Aplicação de Criptografia de Dados em um Ambiente Corporativo

Clodoaldo Júnior, Alex Feleol

Fundação Centro de Análise, Pesquisa e Inovação Tecnológica – FUCAPI

CEP 69075-351 – Manaus – AM – Brazil

{cdinizpj@gmail.com , alexfeleol@msn.com}

Abstract. *Currently, many security mechanisms are applied in the protection of strategic information for public and private organizations. However, these organizations remain vulnerable, owing to the large amount of sensitive information that travels into your computer network. The vulnerability results from the minimization of security mechanisms applied to an intranet, making this environment conducive to a passive attack, exploiting the communication between a machine origin and a destination machine, violating the principle of confidentiality. The purpose of this article is to demonstrate the vulnerability to exchange information on a local area network (intranet) and present an encryption model, focused on data security, transferred this way of communication, establishing a secure channel between sender and receiver in order to mitigate information capture attacks. A software was developed and adapted to demonstrate effectively the use of cryptographic techniques of symmetric algorithms, particularly the AES (Advanced Encryption Standard).*

Resumo. *Atualmente, inúmeros mecanismos de segurança, são aplicados na proteção das informações estratégicas de organizações públicas e privadas. No entanto, essas organizações continuam vulneráveis, em virtude à grande quantidade de informação sigilosa que trafegam em sua rede de computadores. A vulnerabilidade é decorrente da minimização de mecanismos de segurança aplicados à uma intranet, tornando esse ambiente propício à um ataque passivo, explorando a comunicação entre uma máquina origem e uma máquina destino, violando o princípio da confidencialidade. O objetivo deste artigo é demonstrar a vulnerabilidade na troca de informações em uma rede local (intranet) e apresentar um modelo de criptografia, voltado para segurança dos dados, transferidos neste meio de comunicação, estabelecendo um canal seguro entre emissor e receptor, a fim de mitigar os ataques de captura de informações. Um software foi desenvolvido e adaptado, para demonstrar de forma efetiva a utilização das técnicas criptográficas de algoritmos simétricos, em especial do AES (Advanced Encryption Standard).*

1. Introdução

A segurança da informação é essencial nos dias de hoje, principalmente quando notamos o uso crescente de serviços como *Home*/*Internet Banking*, comércio on-line, videoconferências, transferências (receber e enviar) de arquivos, acesso a redes sociais, dentre outros. De acordo com Nakamura e Geus (2007), os principais ataques a furtos

de informações, ocorrem na rede interna (*intranet*) da empresa, onde normalmente as técnicas aplicadas à segurança da informação são minimizadas.

O ataque pode ocorrer através de scripts executados de forma programada a partir de um computador, de um laptop ou qualquer outra tecnologia (ativo) que esteja conectado na rede ou acionado diretamente por um usuário mal-intencionado. Um dos pilares da segurança da informação, o ser humano, muitas vezes é responsável diretamente pelo fato, onde, sendo passível de instintos e desejos, pode contribuir para desencadear o processo de furto de dados de uma empresa.

Com base nesse cenário, um software foi desenvolvido e adaptado, aplicando processos técnicos existentes de criptografia de dados na proteção de informações que trafegam no ambiente coorporativo (cooperativo) mitigando o furto de informações.

Este artigo está organizado em mais quatro seções. Na seção 2, denominada "Metodologia", é abordada a vulnerabilidade de um ambiente corporativo (cooperativo), vislumbrando cenários reais de furto de informações, bem como, propor técnicas de proteção a ser utilizadas no desenvolvimento do software, através dos aspectos de segurança estudados, durante a elaboração deste trabalho. Na seção 3, denominado "Estudo de Caso", contém o cenário de experimentação que o aplicativo desenvolvido foi submetido, descrevendo os testes realizados, com as implementações do algoritmo criptográfico *AES* (*Advanced Encryption Standard*). A seção 4 apresenta os resultados obtidos com a apresentação dos resultados provenientes da transferência de informações no ambiente corporativo (cooperativo), através de um chat interno. As conclusões e as perspectivas são abordadas nas seções de número 5 e 6 respectivamente.

2. Metodologia

Nesta seção pretende-se apresentar a metodologia empregada para o desenvolvimento do estudo de caso e o conjunto ferramental tecnológico utilizado.

2.1 Problemas e Riscos no Ambiente Corporativo (Cooperativo)

Diversas organizações trocam informações técnicas, comerciais e financeiras com suas filiais, parceiros comerciais, fornecedores, clientes, e até mesmo com usuários móveis através de uma rede heterogênea totalmente integrada. Esse ambiente integrado é denominado de ambiente corporativo (cooperativo). Esse ambiente implica cuidados para evitar pontos de brechas em segurança, os quais se tornam grandes desafios para os administradores de rede, principalmente quando envolve complexidade dos níveis de acesso.

De acordo com Stallings (2008), devido o ambiente corporativo ser interligado por meio de redes locais, é possível alcançar outras estações de trabalhos e servidores na mesma rede. Esse simples fato, caracteriza uma vulnerabilidade, já que um intruso pode monitorar o tráfego na rede local capturando o conteúdo desejado. E ainda, se parte da rede possuir tecnologia sem fio, o potencial de interceptação das informações é muito maior.

O estudo desse trabalho foi baseado no termo inglês, *insiders*, que consiste naquele indivíduo que utiliza a rede da empresa, com perfil de um colaborador (contratado ou terceirizado) ou de um parceiro comercial (cliente, fornecedor, distribuidor, etc.).

2.2 Segurança da Informação

Devido ao universo complexo em que é estabelecido, a segurança de um ambiente corporativo (cooperativo), envolve a criação de um perímetro de segurança e o planejamento de defesa contra possíveis ataques a seus computadores com a finalidade de mitigar, roubo de identidades, captura de dados bancários e cartões de crédito, dentre outros. Goodrich e Tamassia (2008), conceitua os 03 pilares da segurança da informação:

Confidencialidade: Evita a revelação não autorizada da informação, ou seja, somente permite acesso ao conteúdo da informação, àquela pessoa autorizada a tê-la.

Integridade: Evitar que uma informação possa ser alterada sem prévia autorização;

Disponibilidade: Consiste que a informação esteja acessível e utilizável, ou ainda, possa ser modificada por usuários autorizados quando necessitarem.

2.2.1 Engenharia Social – Um Ataque à Segurança

Diversos ataques de engenharia social, utilizam os *insiders* como forma de subtrair informações da rede interna de uma organização. Esses indivíduos podem comprometer a organização, estudando hábitos, pontos fracos, vulnerabilidades visíveis, que podem ser explorados em outro momento. Abaixo, é relatado um caso real de furto de informações confidenciais dentro de organizações:

Um dossiê contendo segredos de novas tecnologias aplicadas aos carros de fórmula 1, da equipe Ferrari, foi furtado por um membro da sua própria equipe. Consta ainda que, um dos principais motivos para a ocorrência do fato, deveu-se a insatisfação com o cargo que o individuo exercia na escuderia, no dado momento da realização do furto (VEJA, 2007).

2.3 Criptografia

De acordo com Coulouris, Dollimore e Kindberg (2007), muitos mecanismos de segurança são baseados em criptografia de chave pública (simétrica) em nível de *software*. Pelo fato de utilizar a mesma chave tanto para cifrar como para decifrar, possue caracteristicas de grande poder computacional e velocidade na execução dos processo criptográficos. É largamente utilizada, em emails, arquivos em geral, banco de dados, dentre outros.

2.3.1 Algoritmo Criptográfico - *Rijndael*

Para Moreno, Pereira e Chiaramonte (2005), devido a necessidade de rever o padrão de criptografia oficial utilizado na segurança das aplicações comerciais, o governo americano, solicitou à comunidade cientifica, que apresentasse um novo padrão de criptografia simétrica, denominado de *Advanced Encryption Standard* (*AES*) operando com blocos de 128 bits, utilizando chaves de 128, 192 e 256 bits. O *Rijndael* foi escolhido por ter sido o mais efeciente, dentre os 21 algoritmos, submetidos ao *National Institute of Standards and Technology* (*NIST*).

2.3.2 Matemática do Algoritmo *Rijndael*

No *Rijndael* são definidos dois tipos de operações: uma a nível de byte e outra a nível de palavras. O nível de byte é representado por um elemento de campo finito GF(2^8). A

nível de palavras, as operações são definidas em conjuntos de 4 *bytes*. Representado como um polinômio p(x) de grau sete com coeficiente {0,1}, como descrito a seguir:

$$p(x) = b_7x^7 + b_6x^6 + b_5x^5 + b_4x^4 + b_3x^3 + b_2x^2 + b_1x^1 + b^0$$

a) Operação de Soma – polinômio cujo coeficientes é resultante da soma do modulo 2 dos coeficientes dos termos.

Exemplo: Soma dos bytes: 01010111 = $x^6 + x^4 + x^2 + x^1 + x$ e 10000011 = $x^7 + x + 1$ resulta em: $\boldsymbol{x^7 + x^6 + x^4 + x^2}$

b) Operação de Multiplicação – Diferente da operação de adição, a operação com multiplicação, sempre terá como resultado um polinômio de grau inferior a 8. É representado na forma de *m(x)* e é dado por:

$$m(x) = x^8 + x^4 + x^3 + x + 1$$

2.3.3 Processo de Cifragem do *Rijndael*

Um dos principais processos que tornou o *Rijndael*, forte, contra ataques criptoanalíticos, é o processo de transformação, onde os bytes de cada bloco são substituidos por seus equivalentes em um processo não-linear por meio de uso de uma S-BOX, onde a finalidade, é que não exista um ponto fixo e nem um ponto inverso.

A mesma é construída em tempo de execução e é calculada da seguinte forma (Terada, 2008):

- Inicializa cada linha de uma matriz com 256 valores sequenciais crescentes de 0 a 255.
- Substitue cada *byte* nesta matriz pelo seu inverso em $GF(2^8)$ módulo *m(x);*
- aplica-se em seguida, uma multiplicação matricial seguindo a tabela 1, abaixo:

Tabela 1. Multiplicação matricial

$$\begin{vmatrix} y_0 \\ y_1 \\ y_2 \\ y_3 \\ y_4 \\ y_5 \\ y_6 \\ y_7 \end{vmatrix} = \begin{vmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 \\ 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 \end{vmatrix} \begin{vmatrix} b_0 \\ b_1 \\ b_2 \\ b_3 \\ b_4 \\ b_5 \\ b_6 \\ b_7 \end{vmatrix} \oplus \begin{vmatrix} 1 \\ 1 \\ 0 \\ 0 \\ 0 \\ 1 \\ 1 \\ 0 \end{vmatrix}$$

Abaixo, foi reproduzido no quadro 1, a tabela S-BOX calculada, utilizada no processo de transformação, onde, os bytes de cada bloco são substituidos por seus equivalentes em um Corpo de Galois[1] GF (2^8).

Quadro 1. S-BOX

		Y															
		0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
	0	63	7C	77	7B	F2	6B	6F	C5	30	01	67	2B	FE	D7	AB	76
	1	CA	82	C9	7D	FA	59	47	F0	AD	D4	A2	AF	9C	A4	72	C0
	2	B7	FD	93	26	36	3F	F7	CC	34	A5	E5	F1	71	D8	31	15
	3	04	C7	23	C3	18	96	5	9A	07	12	80	E2	EB	27	B2	75
	4	09	83	2C	1A	1B	6E	5A	A0	52	3B	D6	B3	29	E3	2F	84
	5	53	D1	00	ED	20	FC	B1	5B	6A	CB	BE	39	4A	4C	58	CF
	6	D0	EF	AA	FB	43	4D	33	85	45	F9	02	7F	50	3C	9F	A8
X	7	51	A3	40	8F	92	9D	38	F5	BC	B6	DA	21	10	FF	F3	D2
	8	CD	0C	13	EC	SF	97	44	17	C4	A7	7E	3D	64	5D	19	73
	9	60	81	4F	DC	22	2A	90	88	46	EE	B8	14	DE	5E	0B	DB
	A	E0	32	3A	0A	49	6	24	5C	C2	D3	AC	62	91	95	E4	79
	B	E7	C8	37	6D	8D	D5	4E	A9	6C	56	F4	EA	65	7A	AE	08
	C	BA	78	25	2E	1C	A6	B4	C6	E8	DD	1F	1F	4B	BD	8B	8A
	D	70	3E	B5	66	48	03	F6	0E	61	35	B9	B9	86	C1	1D	9E
	E	E1	F8	98	11	69	D9	8E	94	9B	1E	E9	E9	CE	55	28	DF
	F	8C	A1	89	0D	BF	E6	42	68	41	2D	0F	0F	B0	54	BB	16

2.4 Trabalhos Relacionados

Com a finalidade de enriquecer o embasamento teórico, foram pesquisados assuntos relacionados no campo de atuação deste trabalho. Dentre eles, destacam-se os trabalhos relacionados a seguir:

No estudo apresentando por Alves (2011), intitulado "Política de Segurança da Informação: Análise ergonômica da difusão das normas em uma organização pública e seu impacto nos comportamentos inseguros", alerta que a engenharia social, consiste em ações efetuadas para obter acesso a informações sensíveis das organizações e/ou sistemas por meio da persuasão ou exploração da confiança das pessoas. Enfim, todos,

[1] Corpo finito com dois elementos, 0 e 1 (Terada, 2008).

os escalões de colaboradores da empresa, precisam ter um treinamento em segurança, para que possam mitigar esse tipo de ataque.

Em uma dissertação de mestrado, Pigatto (2012), "Segurança em Sistemas Embarcados críticos - utilização de criptografia para comunicação segura", explica o desempenho de um dos algoritmo de criptografia, o *AES*, utilizado em um estudo de caso, sobre aplicação de cifragem de dados para dificultar que usuários não autorizados sejam capazes de furtar informações no ambiente de comunicação na utilização de sistemas embarcados.

Em outro estudo, apresentado por Souza (2010), "Segurança para Web Services com criptografia heterogênea baseada em Proxy", abrange o uso de criptografia simétrica e assimétrica como sendo necessários para manter um sistema seguro, principalmente, quando a comunicação acontece em uma rede não segura, como a internet.

3. Estudo de Caso

Este estudo de caso é composto de um cenário experimental, para aplicabilidade de testes, realizando transferências de dados no ambiente coorporativo (cooperativo), citado na seção 2, e em seguida, aplicar proteção através de criptografia simétrica para provimento de comunicação segura.

3.1 Cenário

O cenário experimental projetado como laboratório de testes, tem como objetivo aplicar a metodologia proposta, no modelo de um ambiente corporativo (cooperativo) desprotegido, visualizado na figura 1. Foi definido a seguinte especificação de identificação das máquinas no cenário aplicado: Computador Servidor - *IP*: 10.1.141.23 e demais computadores cliente: CJunior com o *IP*: 10.1.141.99 e JDiniz com o *IP*: 10.1.101.163 como máquinas clientes.

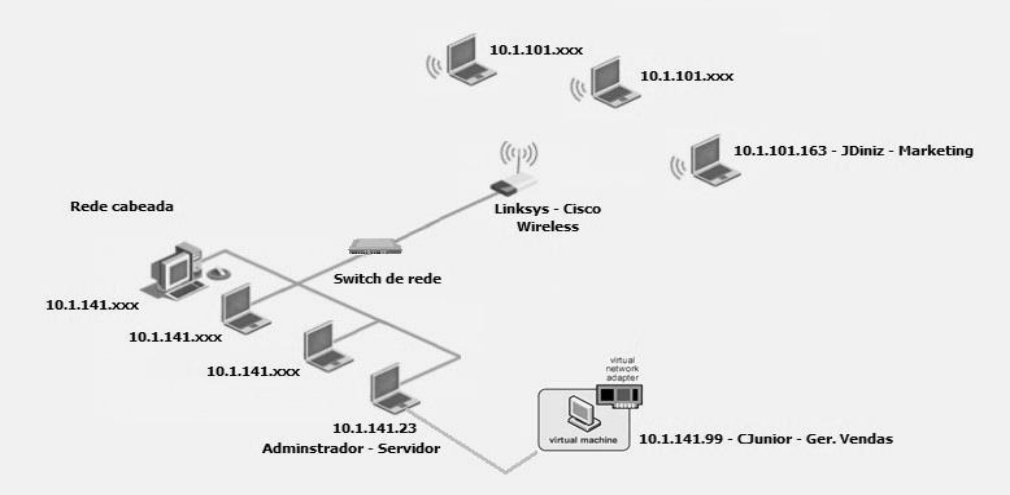

Figura 1. Cenário para aplicação de testes

3.2 Execução dos Testes

Foi realizado um diálogo em chat interno, entre duas entidades forte do ambiente corporativo (cooperativo), JDiniz - Gerente de Marketing e CJunior - Gerente de Vendas, indagados pelo Administrador de TI.

Nesse contexto, são reveladas ações de um aparente lançamento de um novo produto comercial, que devido a uma vulnerabilidade de segurança na rede interna, um intruso pode escutar a rede e capturar dados que permitam ter o conhecimento do teor do diálogo entre os envolvidos. A figura 2 visualiza, o diálogo entre emissor e receptor.

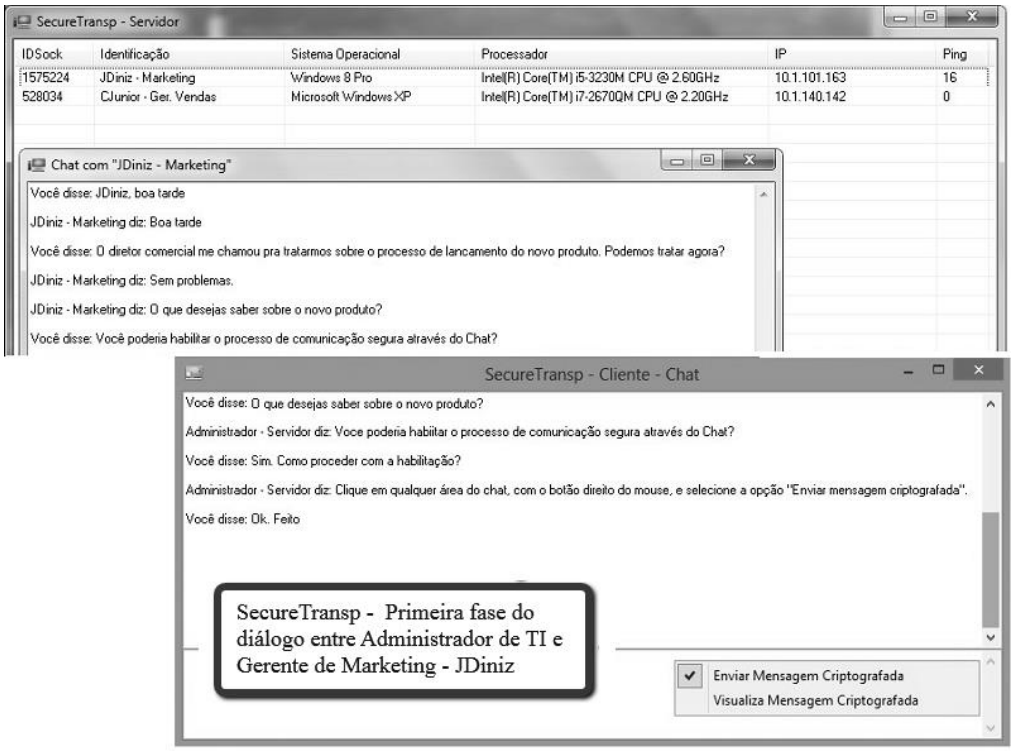

Figura 2. Primeira fase do diálogo entre Administrador de TI e JDiniz

O que motivou os estudos realizados neste presente trabalho é visualizado a seguir, através da captura de fragmentos do diálogo no ambiente corporativo (cooperativo) simulado, entre o Administrador de TI e o gerente de Vendas, CJunior. Essa captura de pacotes, é mostrado na figura 3.

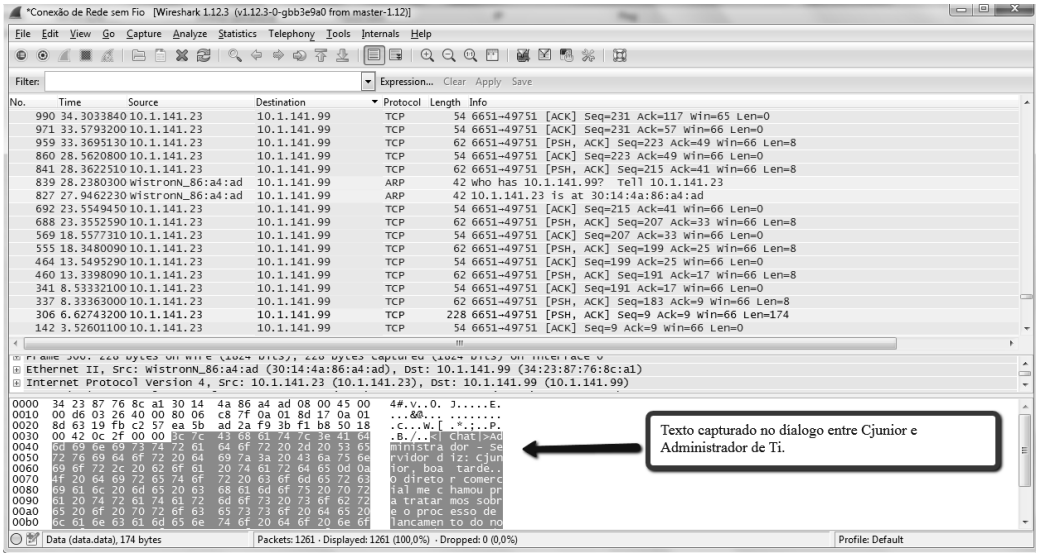

Figura 3. Captura do diálogo entre emissor e receptor no ambiente

É visível notar, na figura 3, o monitoramento da rede por meio do *wireshark*[2] (*sniffer de rede*), a intrusão de um *insider* atuando como *man-in-the-middle*[3].

Em uma segunda parte do diálogo, o Administrador de TI, habilita a comunicação segura no *software*, enviando uma mensagem à JDiniz, solicitando ao mesmo, verificar se a mensagem foi enviada criptografada.

É salutar deixar claro que, esse procedimento, é somente para demonstrar que o canal está seguro, ou seja, entre o emissor e o receptor, quando do envio da mensagem, percorre entre origem e destino, somente a mensagem criptografada.

A composição dos textos é uma funcionalidade do *software*, para que o usuário cliente possa confirmar o seu recebimento criptografado. Após, essa confirmação o usuário pode desabilitar a visualização da mensagem criptografada, a fim de receber somente as mensagens livres.

A figura 4 visualiza a segunda fase do diálogo entre Administrador de TI e JDiniz, bem como, o item "Visualiza mensagem criptografada", disponível somente na versão cliente do *software*.

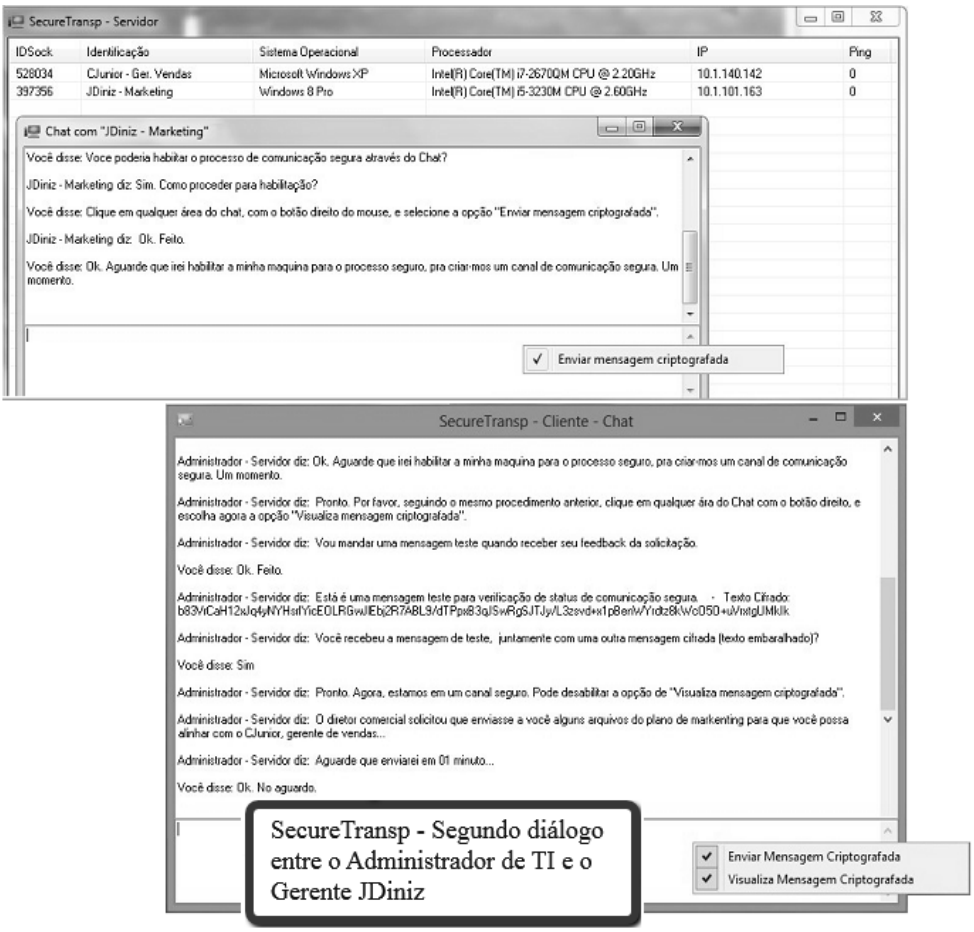

Figura 4. Segunda fase do diálogo entre Administrador de TI e JDiniz

[2] Denominado também de *sniffer* (farejador), é um analisador de protocolo que permite capturar o tráfego em uma rede de computadores.

[3] *Man-in-the-middle* (homem do meio) - ataque de captura de pacotes entre emissor e receptor, por terceiros.

4. Resultados Obtidos

Na seção anterior, após ser habilitado a comunicação segura no software cliente, o *insider*, realizou uma nova captura na rede local, obtendo novamente sucesso. Entretanto, o canal de comunicação entre emissor e receptor está seguro, conforme mostra a figura 5.

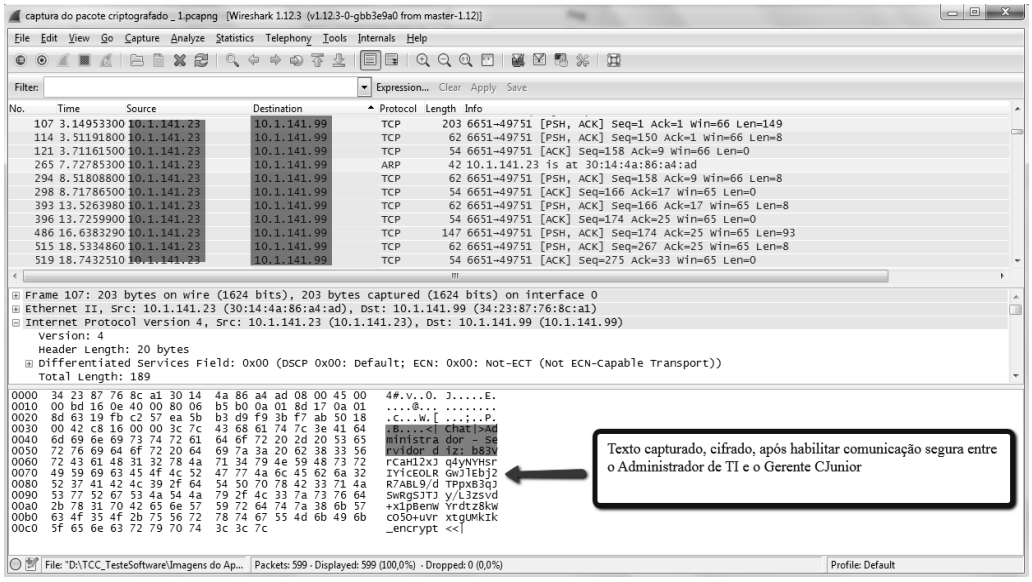

Figura 5. Captura de pacote criptografado

A figura 6 mostra o conteúdo da mensagem legível, que foi criptografada, no envio entre emissor e receptor.

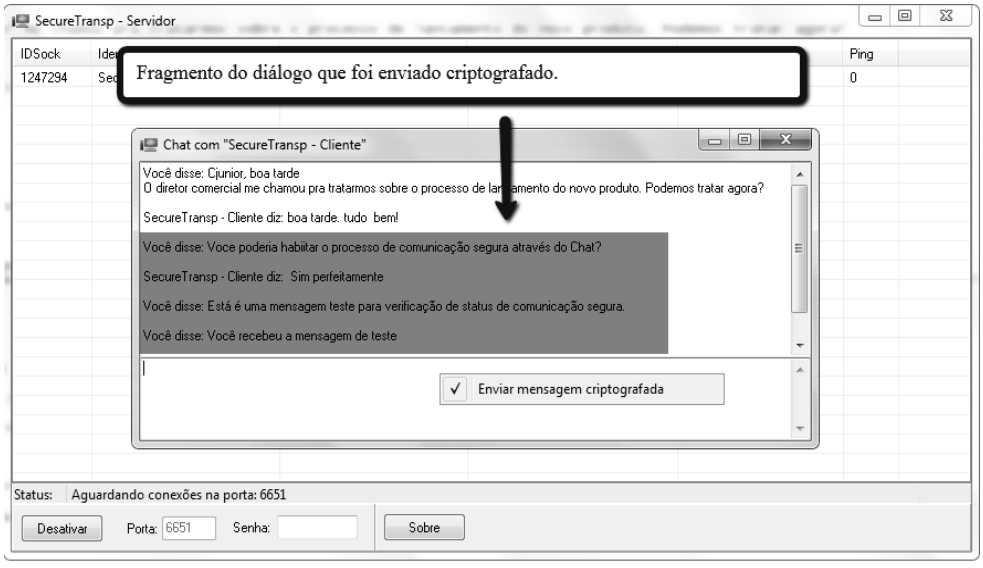

Figura 6. Fragmentos de mensagem legível no *software* cliente

5. Conclusão

Muitos são os tipos de ataque que um ambiente corporativo (cooperativo) pode vir a sofrer, entretanto, com base nos estudos, conceitos e técnicas de criptografia aplicadas, o presente trabalho, demonstrou técnicas simples de criptografia para reduzir a

vulnerabilidade, em pelo menos, um deles, disponibilizando assim, um cenário ideal para troca de informações, mitigando o sucesso de ataques nesse ambiente.

A proteção por perímetro não resolve todos os problemas, ou ainda, que tenha maior relevância sobre os demais, porém, com o auxílio de outras técnicas, processos e políticas de segurança, é possível abranger uma amplitude maior na busca da linha de defesa ideal para uma empresa.

6. Referências

ALVES, Allan Ricardo. **Política de Segurança da Informação: Análise ergonômica da difusão das normas em uma organização pública e seu impacto nos comportamentos inseguros**. 2011. 61 p. Monografia (Especialista em Ciência da Computação: Gestão da Segurança da Informação e Comunicações). Universidade Brasília. Disponível em: http://dsic.planalto.gov.br/documentos/cegsic/monografias_2009_2011/04_Allan.pdf . Acesso em: 04 Set 2014.

COULOURIS, Gerorge. DOLLIMORE, Jean. KINDBERG, Tim. **Sistemas Distribuídos: conceitos e projetos.** Porto Alegre. Bookman. 2007.

GOODRICH, Michael T. TAMASSIA, Roberto. **Introdução à Segurança de Computadores.** Porto Alegre. Bookman. 2013.

MORENO, Edward David. PEREIRA, Fabio Dacêncio. CHIARAMONTE, Rodolfo Barros. **Criptografia em software e hardware**. São Paulo. Novatec. 2005.

NAKAMURA, Emílio Tissaro. GEUS, Paulo Licio de. **Segurança de Redes em Ambientes Cooperativos.** São Paulo. Novatec. 2007.

PIGATTO, Daniel Fernando. **Segurança em sistemas embarcados críticos – utilização de criptografia para comunicação segura**. 2012. 88 p. Dissertação (Programa de Pós-Graduação em Ciência da Computação e Matemática Computacional). Pontifica Universidade Católica do Rio Grande do Sul. Disponível em: www.teses.usp.br/teses/disponiveis/55/.../DanielFernandoPigatto.pdf. Acesso em: 09 Set 2014.

SOUZA, Samuel Camargo de. **Segurança para web services com criptografia heterogênea baseada em Proxy**. 2010. 87 p. Dissertação (Programa de Pós-Graduação em Ciência da Computação da Faculdade de Informática). Pontifica Universidade Católica do Rio Grande do Sul. Disponível em: http://tede.pucrs.br/tde_busca/arquivo.php?codArquivo=2872 . Acesso em: 04 Set 2014.

STALLINGS, William. **Criptografia e Segurança de Redes.** 4. ed. São Paulo. Pearson Prentice Hall. 2008.

TERADA, Routo. **Segurança de Dados: criptografia em redes de computador.** 2. ed. São Paulo. Blucher. 2008.

VEJA. **Espionagem na Fórmula 1**. Veja On-line. Set. 2007. Disponível em: <http://veja.abril.com.br/idade/exclusivo/perguntas_respostas/espionagem_formula1/index.shtml>. Acesso em: 22 novembro 2011.