MARIO ABREU

PREVENÇÃO A FRAUDE EM CARTÃO DE CRÉDITO

SÃO PAULO
2011

MARIO ABREU

PREVENÇÃO A FRAUDE EM CARTÃO DE CRÉDITO

Monografia apresentada na Escola Politécnica da Universidade de São Paulo para conclusão do curso de MBA em Tecnologia da Informação.

Área de Concentração: Tecnologia da Informação

Orientador: Prof. Stephan Kovach

SÃO PAULO
2011

FICHA CATALOGRÁFICA

Abreu, Mario
Prevenção a fraude em cartão de crédito / M. Abreu. -- São Paulo, 2011.
55 p.

Monografia (MBA em Tecnologia da Informação) - Escola Politécnica da Universidade de São Paulo. Programa de Educação Continuada em Engenharia.

1. Tecnologia da informação 2. Fraude 3. Cartão de crédito 4. Redes neurais 5. mineração de dados I. Universidade de São Paulo. Escola Politécnica. Programa de Educação Continuada em Engenharia II. t.

DEDICATÓRIA

Dedico este trabalho a minha esposa Roseli e meus filhos Henrique e Giovanna que com muita paciência, compreensão e carinho me deram condições para concluir este trabalho.

AGRADECIMENTOS

Agradeço a Deus, Jesus Cristo e Santo Expedito que sempre me deram força e esperança para concluir este curso.

Agradeço especialmente ao meu orientador, "Prof. Stephan Kovach" que sempre me apoiou, me ensinou e exigiu de mim a superação para realizar este trabalho.

RESUMO

O presente trabalho trata do tema de prevenção a fraude em cartão de crédito, problema este que tem destaque em notícias dos principais veículos de comunicação e com isto tem se consolidado como uma das principais ameaças à segurança nas transações de cartões.

Em resumo, o presente trabalho ilustra na sua introdução, o tutorial do cartão de crédito, os agentes do cartão de crédito, a operação de autorização e liquidação e os principais canais de distribuição do cartão de crédito. Em seguida são ilustrados os modelos de prevenção a fraude envolvendo redes neurais, mineração de dados, criptografia entre outros. Na penúltima parte do presente trabalho, são citados os pontos fracos na captura de cartões e suas ameaças e vulnerabilidades. Ao final é ilustrada uma alternativa para enrijecer o atual modelo transacional, sugerindo uma proposta baseada em dupla autenticação, onde a primeira parte da senha de autorização pertence ao portador do cartão e a segunda parte é de conhecimento da rede de captura o qual a envia ao portador no instante da transação.

ABSTRACT

This work comes to the topic of credit card fraud prevention, whose problem has been highlighted in major news media and it has been established as a major threat to the security of transactions on cards.

In summary, this study illustrates in its introduction, the tutorial of the credit card, the agents of the credit card, the operation of authorization and settlement and the main distribution channels for credit card. Then are illustrated the models to prevent the fraud involving neural networks, data mining, encryption, among others. In the penultimate part of this study are cited weaknesses in the capture and their threats and vulnerabilities. At the end is illustrated an alternative to stiffen the current transactional model, suggested a proposal based on dual authentication, where the first part of the authorization password belongs to the cardholder and the second part is of knowledge of the network capture which sends it to the cardholder at time of transaction.

LISTA DE ILUSTRAÇÕES

LISTA DE TABELAS

LISTA DE ABREVIATURAS E SIGAS

ABECS	Associação Brasileira das Empresas de Cartões de Crédito e Serviços
ACM	*Association for Computing Machinery*
AES	*Advanced Encryption Standard*
BCB	Banco Central do Brasil
ATM	*Automatic Teller Machine / Any Time Money*
CDA	*Combined Dynamic and Data Authentication*
CVV	*Card Verification Value*
DDA	*Dynamic Data Authentication*
DES	*Data Encryption Standard*
DHKA	Diffie-Hellman *key agreement*
DSA	*Digital Signature Algorithm*
EMV	Europay, Mastercard e Visa
IEEE	*Institute of Electrical and Electronics Engineers*
ISO	*International Organization for Standardization*
KDD	*Knowledge Discovery in Database*
MCP	McCulloch e Pitts
MIME	*Mult-Part Internet Mail Extensions*
OLTP	*Online Transaction Processing*
PCI-DSS	*Payment Card Industry - Data Security Standard*
PIN	*Personal Identification Number*
POS	*Point of Sale* (Ponto de Venda)
RC	*Rivest Ciphers*
RNA	Rede Neural Artificial
RSA	Rivest-Shamir-Adleman
SDA	*Static Data Authentication*
TEF	Transferência Eletrônica de Fundos
URA	Unidade de Resposta Audível
VBS	*Visual Basic Script*
VPN	*Virtual Private Network*

SUMÁRIO

1.0 Introdução

Atualmente o setor financeiro e a população em geral são freqüentemente lesados por fraudadores que se utilizam de métodos, sistemas obscuros e inescrupulosos para realização de fraudes através do sistema transacional de cartões com o objetivo de angariar recursos.

Este tipo de ação criminosa gera prejuízos inestimáveis a população, instituições financeiras e governo.

1.1 Objetivo

Este trabalho tem como objetivo apresentar uma abordagem em relação às fraudes em transações de cartão de crédito, utilizando metodologia de autenticação de dois fatores, com o intuito de agregar segurança e mitigar os riscos de fraude no setor.

1.2 Motivação

Transações financeiras de compra por cartão ocorrem na sua maioria, através de saques e pagamentos em pontos ATM (*Automatic Teller Machine*), pontos de venda (PDV) do comércio e portais on-line através da Internet. Estas modalidades de serviço possuem grande expectativa de crescimento para os próximos anos. Entretanto, devido ao pânico gerado pelas de noticias veiculadas por Ribeiro (2009), Russo [200?] e Jornal Nacional (2009), relatando fraudes relacionadas a cartões de crédito, tornam os usuários destes serviços receosos de sua utilização.

A motivação deste trabalho esta relacionada à necessidade da criação de um novo mecanismo de prevenção para o segmento, que irá proporcionar maior segurança, mitigando os riscos de fraude.

1.3 Estrutura do Trabalho

Este trabalho está organizado como segue:

O capítulo dois aborda o tutorial do tema com uma pequena introdução sobre a história do cartão; os agentes relacionados com transação do cartão de crédito; o

fluxo da operação e liquidação do cartão de crédito; os canais de distribuição transacionais; pontos fracos na captura de transações.

O capítulo três aborda os modelos de prevenção a fraude baseados em RNA (Redes Neurais Artificiais) e Mineração de Dados (*Data Mining*); as tecnologias relacionadas à criptografia e a citação de normas e regras que compõe um ambiente transacional; ameaças e vulnerabilidades identificadas à estrutura de um ambiente transacional; onde ocorrem as fraudes através dos pontos de captura.

O capítulo quatro aborda o atual modelo de autenticação e apresenta uma alternativa para mitigar as vulnerabilidades no sistema, propondo um modelo de autenticação em dois fatores.

Finalizando, o capítulo cinco apresenta a conclusão deste trabalho.

2.0 Tutorial do Cartão de Crédito

Segundo o BCB (2010), o cartão de crédito é o instrumento de pagamento eletrônico de varejo que permite a seu portador adquirir bens e serviços nos estabelecimentos credenciados, além de possibilitar a realização de saques nos caixas automáticos da rede conveniada. Para tal, o portador dispõe de um limite de crédito para cobrir despesas de compras e saques em espécie.

Em geral, o cartão de crédito é adquirido junto a um banco que, em parceria com as administradoras de cartões, gerencia a sua venda, efetua a entrega ao portador, gerencia o crédito e faz a cobrança das faturas. O cartão também pode ser oferecido diretamente pela administradora.

A relação jurídica entre o emissor do cartão e o portador é a regida por um contrato de adesão. Na avaliação da solicitação do cartão de crédito, feita pela administradora do cartão ou pelo banco emissor, é utilizada metodologia de pontuação, que busca mensurar, principalmente, a capacidade de pagamento do proponente. Com base nos resultados (pontos), é tomada a decisão quanto à emissão do cartão e, se aprovado é estabelecido o limite de crédito correspondente.

Segundo a Associação Brasileira das Empresas de Cartões de Crédito e Serviços, em 1950, foi emitido o primeiro cartão denominado Diners Club Card, que passou a ser aceito como meio de pagamento em 27 (vinte e sete) restaurantes.

Em 1952, o conceito de cartão ganhou novos adeptos, onde ocorreu à emissão do primeiro cartão de validade internacional. Sua rede afiliada já abrangia um grande número de restaurantes, hotéis e diversos estabelecimentos varejistas. Por volta de 1960 o cartão foi aceito em mais de 50 países em todos os continentes.

Em 1966, o Bank American Service Corporation lançou com êxito o Bank Americard, sendo que mais tarde originou a bandeira Visa. Na mesma época a American Express criou um cartão semelhante ao Diners Club, para uso em hotéis e restaurantes.

2.1 Agentes do Cartão

De acordo com MasterCard, o Cartão tem definidos cinco agentes envolvidos em sua operação de funcionamento, como segue abaixo:

a) Portador (*Cardholder*): É o proprietário do cartão, responsável contratual e juridicamente pelo cartão, mesmo em casos em que há dependentes (cartões adicionais).
b) Credenciado / Comerciante (*Merchant*): É o termo usado para identificar o estabelecimento ou empresa que aceita determinado cartão de crédito.
c) Adquirente (*Acquirer*), É a instituição financeira ou organização que presta serviços de processamento de cartão para o lojista, também é responsável pelo credenciamento, gerenciamento e relacionamento entre as bandeiras de crédito e débito e os estabelecimentos comerciais.
d) Cartão de Associação / Bandeira (*Card Association / Brand*): É a marca do cartão e opera um mediador entre o adquirente e o emissor de autorização de operação e financiamento. Responsável por definir as regras do cartão, as bandeiras precisam se associar aos emissores (bancos) de cartões para que o financiamento do cartão aconteça.
e) Emissor (*Issuer*): É a instituição financeira ou organização que emitiu o cartão de crédito para o titular do cartão. Também é a empresa administradora do cartão. Em geral são os bancos e as empresas prestadoras de serviços que emitem e gerenciam o cartão de crédito. O emissor é quem, de fato, financia o crédito do cartão e quem estabelece a taxa de juros e os limites de crédito.

2.2 Operação de Autorização e Liquidação de Cartão de Crédito

A Figura 2.2, ilustra o fluxo básico de autorização e liquidação nas transações de Cartão de Crédito, demonstrando os cinco agentes envolvido no processo.

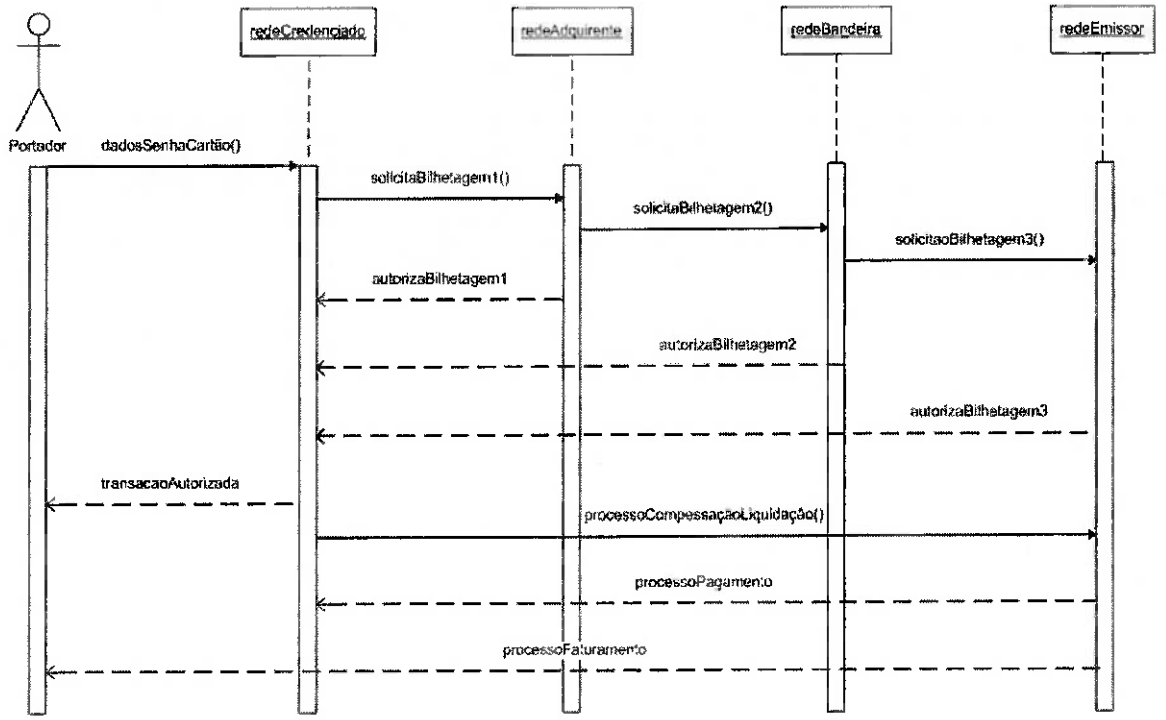


Figura 2.2 – Fluxo básico de autorização e liquidação de transações.

Ainda de acordo com MasterCard, este fluxo é conhecido como "intercâmbio", e consiste em algumas etapas:

a) Autorização: De posse do cartão, o "Credenciado" inicia a transação enviando os dados do "Portador" para o "Adquirente", este por sua vez realiza testes de fraude, bilheta a transação e encaminha para "Bandeira". A "Bandeira" checa e bilheta a transação, efetua autorização e encaminha os dados para o "Emissor". O emissor valida a transação e em seguida autoriza o processamento da transação para o Portador do cartão e o "Credenciado".

b) Lotes: Após a aprovação da transação, o sistema armazena as informações em um lote para processamento posterior (normalmente no final do dia), informações deste lote são encaminhadas para "Credenciado", "Adquirente", "Bandeira" e "Emissor".

c) Compensação e Liquidação: Os lotes são submetidos a processamento da "Bandeira" e o "Emissor" que por conseqüência emite a fatura para o "Portador" com os débitos das transações ocorridas no período.

d) Financiamento: Uma vez que o "Adquirente" tenha sido pago, o "Credenciado" recebe o pagamento. O montante que o "Credenciado" recebe é igual ao valor da transação, menos a taxa de desconto, que é a taxa paga ao "Adquirente" pelo processamento da transação.

2.3 Canais de distribuição

De acordo com BCB (2010), os canais de distribuição são os diversos mecanismos e dispositivos que possibilitam a utilização dos instrumentos de pagamento e a realização de operações bancarias tais como saques, depósitos, pagamentos, transferências, consultas e outros serviços.

Os principais canais de distribuição dos instrumentos de pagamento são as agências bancárias, as redes de ATM, as redes de terminais de transferência eletrônica de fundos (TEF) existentes nos pontos de venda (POS), conhecidas como redes de POS, e as redes de acesso remoto (computadores pessoais, telefone, etc.)

Do ponto de vista da utilização dos instrumentos de pagamento, as agências bancárias, os postos de atendimento e os correspondentes bancários são canais de distribuição destinados, em geral, a cheques e a transferências de crédito. Redes de ATM e acesso remoto cumprem essa mesma função com relação às transferências de crédito e aos débitos diretos. As redes de POS permitem o acesso às transações com os cartões de pagamento.

No Brasil, o fornecimento de serviços de canais e redes de distribuição é realizado por intermédio das instituições financeiras, das administradoras de cartões de pagamento e das empresas de tecnologia bancária.

A Figura 2.3, ilustra alguns dos principais elementos de distribuição existentes atualmente, entretanto por motivos de segurança e confidencialidade, detalhes de conectividade e a fonte destas informações não podem ser divulgados:

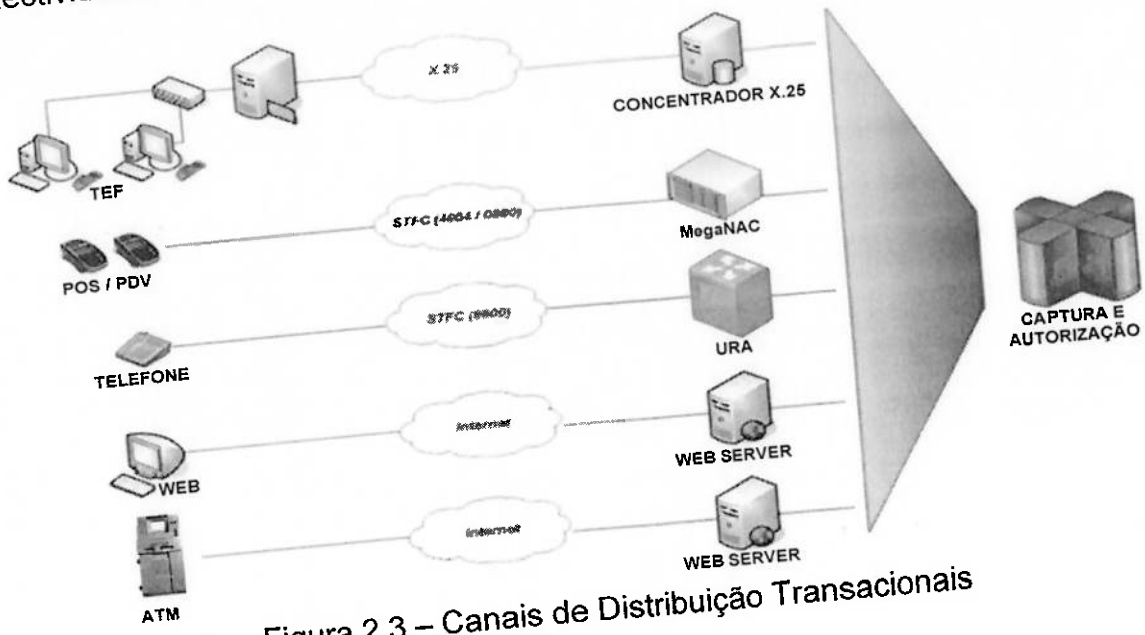


Figura 2.3 – Canais de Distribuição Transacionais

a) TEF: De acordo com BCB (2010), TEF (Transferência Eletrônica de Fundos), é um equipamento composto por um computador padrão, impressora fiscal, links de comunicação e software de *check-out*, que realiza a captura eletrônica e processamento de transações através do concentrador TEF. O concentrador TEF é o sistema responsável por receber, dos caixas ou *check-outs*, as transações e encaminhá-las para cada bandeira. É um equipamento destinado a grandes estabelecimentos que possuem vários *check-outs* interligados em rede e com grande volume de transações. Utiliza circuito X.25 e concentrador X.25 para envio das informações a rede transacional.

b) POS/PDV: De acordo com Hipercard, POS/PDV (*Point Of Sale* ou Ponto De Venda) é um equipamento eletrônico de captura e transmissão de dados de transações, que utiliza linha de telefonia convencional para comunicação. É um elemento destinado a estabelecimentos comerciais de pequeno e médio porte que apresentem os requisitos básicos de infra-estrutura para utilização, tais como linha telefônica convencional e ponto de energia. Este meio utiliza

linha discada telefônica ou *link* de banda larga para realizar captura e autorização.

c) Telefone: Ou (meio de captura com teclado liberado), segundo Hipercard, é uma modalidade de venda nos meios de captura POS ou PDV em que a transação é efetuada sem a presença física do cartão. Este recurso é destinado a estabelecimentos comerciais que necessitam realizar suas vendas através da digitação dos dados do cartão. Este meio utiliza linha telefônica para realizar captura e autorização.

d) WEB – São transações eletrônicas de compra e venda com a utilização de cartão de crédito através da Internet. É conhecido no mundo digital como *e-commerce*. Utiliza linha discada telefônica ou *link* de banda larga através da internet para realizar captura e autorização.

e) ATM - De acordo com BCB (2010), os terminais ATM são equipamentos eletromecânicos, de auto-atendimento, que permitem a seus usuários, por meio do uso de um cartão a realização de saques, pagamentos, transferências, consultas e outras operações bancárias. Este meio utiliza *link* de comunicação dedicado para realizar captura e autorização.

2.4 Pontos Fracos na Captura de Transações

De acordo com Burton, Chuvakin, Elberg, Freedman, King, Paladino e Shcooping (2007), a Figura 4.1 ilustra a topologia detalhada de uma rede transacional baseada nos padrões PCI. Ainda nesta figura estão destacados os pontos de captura como possíveis ameaças a o ambiente.

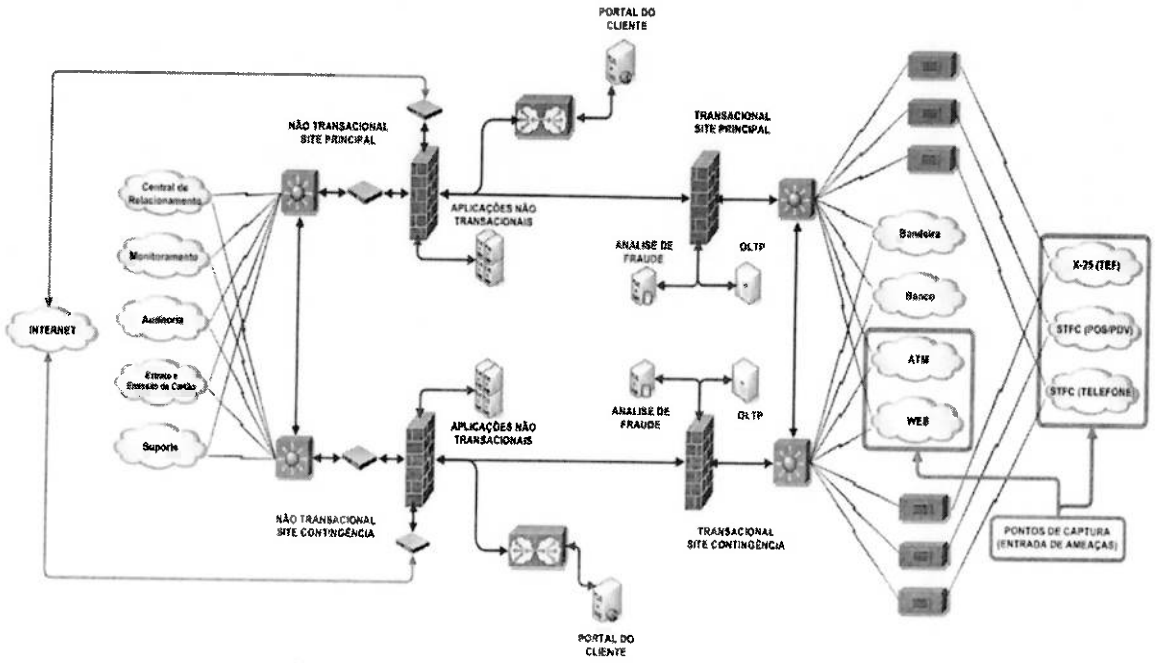


Figura 4.1 – Topologia Rede Transacional

De acordo com Sambray, McClure e Kurtz (2002), os pontos de fragilidade de uma rede se concentram principalmente nas entradas de dados. A Figura 4.1 destaca estes pontos através dos quadros grafados em vermelho. As demais entradas tratam de informações institucionais, não transacionais e internet.

No centro desta topologia, pode ainda ser observada a conexão com serviços de OLTP (*Online Transaction Processing*) e serviços de análise de fraudes já abordados no Capítulo três deste trabalho.

3.0 Modelos de Detecção a Fraude e as Ameaças Transacionais

De acordo com artigos de Chan, Fan, Prodromidis e Stolfo (1999), Ma e Li (2009), Pejic-Bach (2010), Richardson (1997), podemos constatar que as principais técnicas de detecção de fraudes são baseadas em Redes Neurais Artificiais (RNA) e Mineração de Dados (*Data Mining*) sendo que as duas técnicas podem ser utilizadas em conjunto e também podem ser acrescidas de metodologias estatísticas para obtenção de resultados.

3.1 Redes Neurais Artificiais (RNA)

De acordo com Santos (2011), o uso de redes neurais artificiais (RNA) já está presente em diversos segmentos: Na indústria, automatizando ou otimizando partes de processos produtivos; Em segurança de sistemas informatizados, atuando, por exemplo, em "*firewalls* inteligentes", detectando e frustrando tentativas de invasão a redes de computadores. Redes Neurais também estão sendo utilizadas amplamente pelo mercado financeiro em aplicações como: medição de riscos de crédito, estratégia de cobrança, detecção de fraudes, previsão de riscos de sinistros e até para antecipar tendências em bolsas de valores e mercadorias.

De acordo com Braga, Carvalho e Ludermir (2000), uma RNA é baseada em um neurônio biológico que dispara quando a soma dos impulsos que ele recebe ultrapassa o seu limiar de excitação (*threshold*). O corpo do neurônio é emulado por um mecanismo simples que faz a soma dos valores recebidos pelo neurônio (soma ponderada) e decide se o neurônio deve ou não disparar (saída igual a 1 ou a 0) comparando a soma obtida ao limiar ou *threshold* do neurônio. No modelo MCP (McCulloch e Pitts), a ativação do neurônio é obtida através da aplicação de uma "função de ativação", que ativa ou não a saída, dependendo do valor da soma ponderada das suas entradas. Na descrição original do modelo MCP, a função de ativação é dada pela função de limiar que é ilustrada na equação abaixo:

$$\sum_{i=1}^{n} xi\, wi \geq$$ Onde "θ" é o limiar ou *threshold*

Os pesos determinam "em que grau" o neurônio deve considerar sinais de disparo para uma determinada conexão. Uma descrição do modelo MCP (McCulloch e Pitts) está ilustrada na Figura 3.1

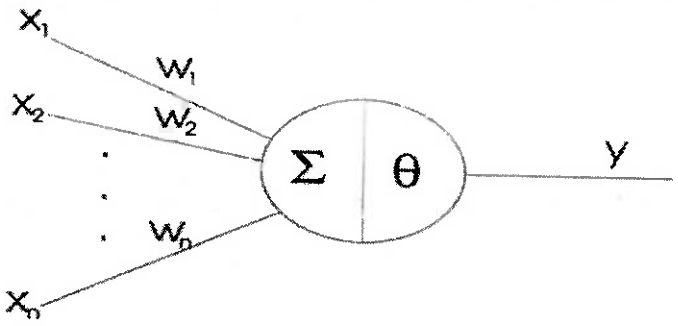


Figura 3.1 – Neurônio de MCP (McCulloch e Pitts)

Baseada no conceito de Braga, Carvalho e Ludermir (2000), a Tabela 3.1.1, ilustra um modelo de análise de perfil em relação ao peso determinado por informações do cliente. As informações aplicadas são baseadas em dados aleatórios para ilustração acadêmica.

Perfil (X)	Entrada	Variável	Risco
	Estado Civil	P1 - Masculino Casado	2
		P2 - Masculino Solteiro	5
		P3 - Feminino Casado	3
		P4 - Feminino Solteiro	6
Peso (W)	Entrada	Variável	Risco
	Renda Mensal	R1 - 0 a 3000 Reais	4
		R2 - 3000 a 6000 Reais	2
		R3 - acima de 6000 Reais	1
	Limite Cartão	L1 - 0 a 3000 Reais	1
		L2 - 3000 a 6000 Reais	4
		L3 - acima de 6000 Reais	8
	Inadimplência	D1 - 0 a 30%	1
		D2 -30 a 80%	4
		D3 -80 a 100%	8
	Valor da Transação	V1 - 0 a 200 Reais	2
		V2 - 200 a 1000 Reais	5
		V3 - acima de 1000 Reais	8

Tabela 3.1.1 – Risco para Perfil (X) / Peso (W)

Na próxima etapa serão considerados os dados acima para simular quatro transações e em seguida calcular o seu grau de risco. Ainda baseada no conceito de Braga, Carvalho e Ludermir (2000), a Tabela 3.1.2 ilustra quatro simulações de transações:

Transação 1					Transação 2					Transação 3					Transação 4			
X	W	Xi	Wi		X	W	Xi	Wi		X	W	Xi	Wi		X	W	Xi	Wi
P4	R1	6	4		P4	R3	6	1		P1	R2	2	2		P3	R2	3	2
P4	L2	6	4		P4	L2	6	4		P1	L1	2	1		P3	L2	3	4
P4	D3	6	8		P4	D1	6	1		P1	D2	2	4		P3	D2	3	4
P4	V3	6	8		P4	V2	6	5		P1	V1	2	2		P3	V2	3	5

Tabela 3.1.2 – Simulação de Transação

Transação 1 = (6x4) + (6x4) + (6x8) + (6x8) = 144

Transação 2 = (6x1) + (6x4) + (6x1) + (6x5) = 66

Transação 3 = (2x2) + (2x1) + (2x4) + (2x2) = 18

Transação 4 = (3x2) + (3x4) + (3x4) + (3x5) = 45

Considerando um *threshold* com limite de risco ≥100, podemos considerar que a "Transação 1" pode se tratar de uma fraude ou possível inadimplência.

Os resultados demonstrados na simulação podem não ser decisivos na aceitação / negação de uma transação. Braga, Carvalho e Ludermir (2000), afirmam que podemos ainda aplicar outras técnicas de comparações seguindo esta mesma linha de raciocínio, uma delas e a técnica de treinamento *perceptron,* onde um sistema computacional pode realizar um aprendizado não supervisionado e aprender com o próprio perfil do usuário o seu modelo de transação. Entretanto para casos que não existe um perfil pré-existente, ou seja, um cliente que não possui o cartão de crédito por um período mínimo para criação de um perfil de análise, os sistemas de detecção de fraude podem considerar esta amostragem como item decisivo.

3.2 Mineração de Dados (*Data Mining*)

De acordo com Abraham, Grosan e Ramos (2006), Mineração de Dados é a aplicação de algoritmos específicos para extração de "padrões" a partir de dados. Os padrões podem ser quaisquer combinações de valores que contêm significado dentro do contexto ou domínio para o qual estão sendo revistos. A "Mineração de Dados" representa o passo principal no processo em "Busca de Conhecimento em Banco de Dados" (*Knowledge Discovery in Database* - KDD) e é descrito de acordo com os seguintes passos:

a) Integração de dados - possibilita a integração de várias fontes de dados incluindo legados e *Data Warehouse*;

b) Seleção e Limpeza de dados - remove dados inconsistentes e fora dos padrões, selecionando somente os dados relevantes para aplicação das técnicas de Mineração de Dados;

c) Transformação de dados - possibilita a transformação ou consolidação dos dados no formato apropriado para o processo de Mineração de Dados;

e) Mineração dos Dados - processo essencial, onde técnicas estatísticas são aplicadas para análise e extração de padrões de dados;

e) Interpretação dos Padrões – identifica os padrões de interesse baseado no resultado apresentado pela "Mineração de Dados". A representação gráfica é uma das técnicas utilizadas para apresentação dos dados obtidos;

f) Conhecimento - Informação para tomada de decisão.

A Figura 3.2 ilustra as etapas do processo de KDD.

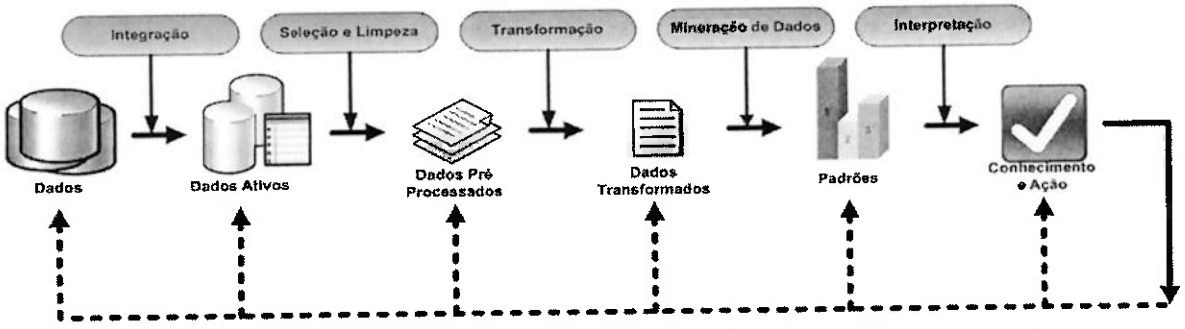


Figura 3.2 – Processo KDD (*Knowledge Discovery in Database*)

De acordo com Fawcett e Provost (1997), o ciclo de aprendizagem de um sistema baseado em KDD é realizado através de regras originadas no conhecimento adquirido através da inclusão de dados. Através da média aritmética e soma ponderada pode ser criado o perfil para analise de resultado. Baseada no conceito de Abraham, Grosan e Ramos (2006), a Tabela 3.2.1 ilustra o modelo de perfil de cliente em um banco de dados para análise através da "Mineração de Dados". As informações aplicadas são baseadas em dados aleatórios para ilustração acadêmica.

Transação	Data	Intervalo	Compra	Localidade	Distância
1	02/01/2009	2	62,00	São Paulo - SP	0
2	05/01/2009	3	56,30	São Bernardo do Campo - SP	20
3	10/01/2009	5	330,30	Ubatuba - SP	210
4	15/01/2009	5	70,00	Angra dos Reis - RJ	280
5	17/01/2009	7	70,00	Rio de Janeiro - RJ	420
6	18/01/2009	1	78,00	Rezende - RJ	270
7	18/01/2009	0	65,00	São Paulo - SP	0
8	24/01/2009	6	542,90	São Paulo - SP	0
9	03/02/2009	10	240,50	São Paulo - SP	0
10	06/02/2009	3	70,00	São Paulo - SP	0
11	10/02/2009	4	135,00	São Paulo - SP	0
12	12/02/2009	2	80,00	São Paulo - SP	0

Tabela 3.2.1 – Perfil de Cliente

Calculo da média aritmética de intervalo (MAI):

$$\bar{X} = \frac{\sum X_i}{n} = \frac{2+3+5+5+7+1+0+6+10+3+4+2}{12} = 4$$

Calculo da média aritmética de compra (MAC):

$$\bar{X} = \frac{\sum X_i}{n} = \frac{62+56,30+330,30+70+70+78+65+542,90+240,50+70+135+80}{12} = 150,00$$

Calculo da média aritmética de distância (MAD):

$$\bar{X} = \frac{\sum X_i}{n} = \frac{20+210+280\ \ 420+270}{12} = 100$$

De acordo com as informações obtidas, podemos criar uma regra para este perfil, levando em consideração 50% de oscilação entre as informações:

SE (2 > MAI > 6) E (75 > MAC > 225) E (50 > MAD > 150) = VERDADEIRO

Ainda baseada no conceito de Abraham, Grosan e Ramos (2006), a Tabela 3.2.2, ilustra o exemplo de transações com possibilidade de fraude, onde os itens de MAI, MAC e MAD estão fora do perfil padrão do exemplo em questão.

Transação	Data	Intervalo	Compra	Localidade	Distância
34	20/06/2010	2	120,00	São Paulo	0
35	20/06/2010	0	80,00	Salvador - BA	2500
36	21/06/2010	1	20,00	Salvador - BA	2500
37	21/06/2010	0	20,00	São Paulo	0
38	21/06/2010	0	20,00	Salvador - BA	2500

Tabela 3.2.2 – Movimentação com indício de fraude

Para definir a confiabilidade ou possibilidade de fraude / inadimplência, um exemplo é a aplicação da técnica da soma ponderada, atribuindo pesos a MAI (Wi) em relação à MAD (Xi), onde:

a) Intervalo 2 / peso = 1;
b) Intervalo 1 / peso = 5;
c) Intervalo 0 / peso = 10.

Ainda baseada no conceito de Abraham, Grosan e Ramos (2006), a Tabela 3.2.3 ilustra a análise de soma ponderada para confiabilidade de transação, baseado em um limiar ou *threshold* ≥100 para casos onde pode ser definido como "Possível Fraude".

Transação	Operação	Status
34	$\sum_{i=1}^{n} X_i W_i = (0X2) = 0$	Confiável
35	$\sum_{i=1}^{n} X_i W_i = (2500X10) = 25.000$	Possível Fraude
36	$\sum_{i=1}^{n} X_i W_i = (2500X5) = 12.500$	Possível Fraude
37	$\sum_{i=1}^{n} X_i W_i = (0X0) = 0$	Confiável
38	$\sum_{i=1}^{n} X_i W_i = (2500X10) = 25.000$	Possível Fraude

Tabela 3.2.3 – Análise de Soma Ponderada

3.3 Criptografia

Os serviços de rede e internet que realizam transações financeiras ou manipulação de informações confidenciais utilizam a criptografia como meio seguro de transporte de dados. Exemplo destes serviços são os sites bancários, comércio eletrônico, entre outros. De acordo com estas informações, podemos considerar que a criptografia de dados é atualmente a maneira mais comum e segura de se transportar informações através da internet.

De acordo com Konheim (2007), Delfs e Knebl (2007), Microsoft Technet (2005) e Suporte Microsoft (2007), existem dois tipos principais de criptografia: Criptografia Simétrica, que também é conhecida como criptografia de chave compartilhada e Criptografia Assimétrica, que também é conhecida como criptografia em duas partes, ou criptografia de chave pública.

Criptografia Simétrica:

A "Criptografia Simétrica" usa a mesma chave tanto para cifrar como para decifrar dados. Os algoritmos que são usados para a criptografia simétrica são mais simples do que os algoritmos usados na criptografia assimétrica. A Figura 3.3.1 ilustra a forma de operação de um algoritmo criptográfico simétrico, onde as chaves que realizam a criptografia da mensagem são idênticas na entrada e na saída da mensagem.

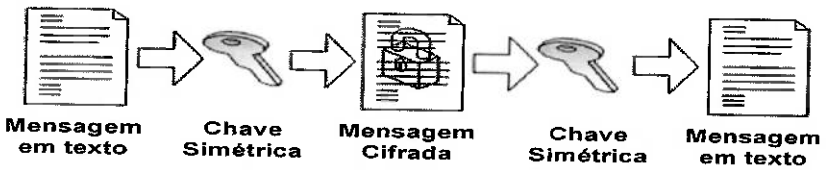


Figura 3.3.1 - Algoritmo Criptográfico Simétrico (Chave secreta)

Uma das principais desvantagens da criptografia simétrica é o uso da mesma chave tanto para cifrar como para decifrar os dados. Por isso, todas as partes que enviam e recebem os dados devem conhecer ou ter acesso à chave de criptografia. Esse requisito cria um problema de gerenciamento de segurança e problemas de gerenciamento de chave que uma organização deve considerar em seu ambiente. O problema de gerenciamento de segurança existe porque a organização provedora deve enviar a chave de criptografia a todos que requererem ou necessitam acesso aos dados criptografados. Os problemas de gerenciamento de chave que uma organização enfrenta, incluem a geração, distribuição, backup, regeneração e ciclo de vida da chave.

A criptografia simétrica fornece autorização para dados criptografados. Por exemplo, ao usar a criptografia simétrica, uma organização pode estar razoavelmente certa de que apenas as pessoas autorizadas a acessar a chave de criptografia compartilhada podem decifrar a mensagem codificada. No entanto, a criptografia simétrica não fornece não-repúdio. Por exemplo, em um cenário em que várias partes têm acesso à chave de criptografia compartilhada, a criptografia simétrica não pode confirmar a origem específica que envia os dados. Os algoritmos de criptografia usados na criptografia simétrica incluem o seguinte: RC2, RC4 e RC5 (RC - *Rivest Ciphers*); 3DES (*Triple Data Encryption Standard*, Padrão triplo de criptografia de dados); AES (*Advanced Encryption Standard*, Padrão de Criptografia Avançada).

Criptografia Assimétrica:

A "Criptografia Assimétrica" usa duas chaves diferentes matematicamente relacionadas para cifrar e decifrar dados. Essas chaves são conhecidas como chaves privadas e chaves públicas. Em conjunto, essas chaves são conhecidas como par de chaves. A criptografia assimétrica é considerada mais segura que a criptografia simétrica, pois a chave usada para cifrar os dados é diferente da chave usada para decifrar. Devido à utilização de algoritmos mais complexos e um par de chaves, o processo de cifrar dados através da criptografia assimétrica é mais lento que o processo de criptografia simétrica. A Figura 3.3.2 ilustra a forma de operação de um algoritmo criptográfico assimétrico, onde um par de chaves é utilizado para realizar a criptografia da mensagem. A informação é cifrada através da utilização da chave pública e decifrada através da utilização da chave privada.

Figura 3.3.1 - Algoritmo Criptográfico Assimétrico (Chave pública)

A criptografia assimétrica permite que somente uma parte detenha a chave privada, essa parte é conhecida como o assunto e as demais partes detêm a chave pública. Os dados cifrados por meio da chave pública só podem ser decifrados pela chave privada. Por outro lado, os dados cifrados por meio da chave privada só podem ser decifrados pela chave pública.

Esse tipo de criptografia fornece autorização quando se usa a chave pública para criptografar dados. Essa chave é disponibilizada publicamente. Desse modo, qualquer um pode criptografar os dados. No entanto, como apenas o assunto mantém a chave privada, este método garante que apenas o destinatário pode decifrar e exibir os dados criptografados.

Esse tipo de criptografia fornece autenticação quando se usa a chave privada para criptografar dados. Apenas o assunto mantém essa chave. No entanto, todos podem decifrar os dados porque a chave pública que decifra esses dados é disponibilizada publicamente. Conseqüentemente, se o destinatário pode decifrar os dados por meio da chave pública, este método garante de que apenas o assunto cifrou os dados. Os algoritmos de criptografia usados na criptografia assimétrica incluem o seguinte: DHKA (*Diffie-Hellman key agreement*); RSA (*Rivest-Shamir-Adleman*); DSA (*Digital Signature Algorithm*, Algoritmo de assinatura digital).

Criptografia Híbrida:

A "Criptografia Híbrida" é um esquema de criptografia em que a criptografia de dados é realizada por meio da combinação de criptografias simétrica e assimétrica.

O método de criptografia híbrida utiliza as forças de ambos os tipos de criptografias para ajudar a assegurar que apenas o destinatário pretendido leia os dados.

Em um cenário de criptografia híbrida, uma organização criptografa os dados usando a criptografia simétrica em conjunto com uma chave gerada aleatoriamente. Essa etapa aproveita a velocidade da criptografia simétrica. Desse modo, a organização criptografa a chave de criptografia simétrica por meio da chave pública de um par de chaves assimétricas. Essa etapa tira proveito da segurança ampliada da criptografia assimétrica. Os dados criptografados, juntamente com a chave simétrica criptografada, são enviados para o destinatário de dados. A Figura 3.3.3 ilustra o processo de criptografia híbrida.

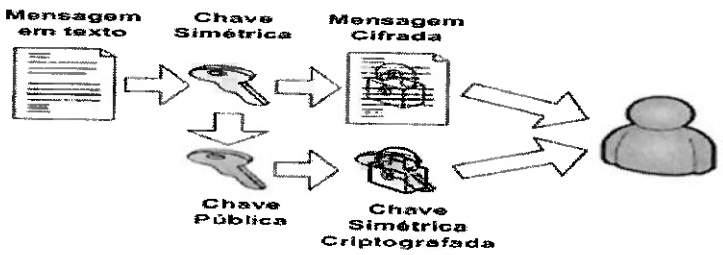


Figura 3.3.3 – Processo de Criptografia Híbrida

Para descriptografar os dados, o destinatário usa primeiramente a chave privada do par de chaves assimétricas para descriptografar a chave simétrica. Em seguida, o destinatário usa a chave simétrica descriptografada para descriptografar os dados. A Figura 3.3.34 ilustra o processo de descriptografia híbrida.

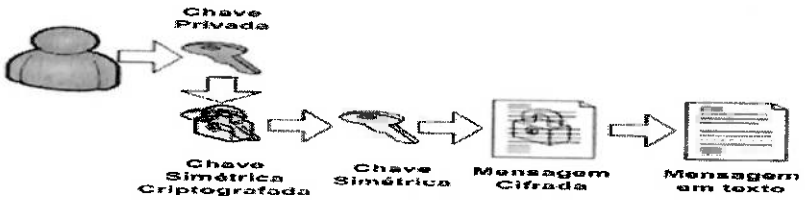


Figura 3.3.4 – Processo de Descriptografia Híbrida.

3.4 Outros Mecanismos

Para disponibilizar confiabilidade, disponibilidade e integridade das informações, Burton, Chuvakin, Elberg, Freedman, King, Paladino e Shcooping (2007) informam que os padrões PCI exigem entre outras necessidades, a implantação de outros mecanismos para prevenção a fraude em redes transacionais, como *Firewalls* inteligentes, IPSs (*Intrusion Prevention System*), autenticação multifator e controle de dados de autenticação após a autorização.

É importante também ressaltar a importância das normatizações do setor, ISO (2003), que alem de outras funções, proporcionam a prevenção de fraude, estão relacionadas à padronização das características físicas do cartão (ISO 7810 e seus derivados) e especificação do intercâmbio entre emissões e aquisições com cartões de crédito (ISO 8583).

3.5 Ameaças e Vulnerabilidade

De acordo com ISO/IEC 27002 os conceitos de ameaça e vulnerabilidade são:

Ameaça - Causa potencial de um incidente indesejado que pode resultar em dano para um sistema ou organização.

Vulnerabilidade - Fragilidade de um ativo ou grupo de ativos que pode ser explorada por uma ou mais ameaças.

De acordo com estas definições, pode ser concluído que qualquer elemento em um ambiente computacional pode ser passível de ameaça ou vulnerabilidade.

3.6 Ameaça por captura em ATM

De acordo com Vamosi (2010), o "*Skimming*" ou golpe do chupa-cabras, é uma forma de fraude financeira que utiliza mecanismos sofisticados de leitura de dados para copiar as informações da fita magnética do cartão de débito ou crédito. Ele pode capturar o número do cartão e a senha denominada como PIN (*Personal Identification Number*).

Para realizar esta ação, o criminoso instala um leitor de fita magnética sobre a fenda existente no caixa eletrônico (ATM). No momento que o usuário insere o cartão, o aparelho efetua a leitura das informações e em seguida aparelho original também

efetua a leitura informações, neste ponto, a transação ocorre como esperado, entretanto o criminoso obtém uma cópia exata dos dados do cartão. Estas informações podem ser transmitidas para o fraudador por *Bluetooth* ou através de telefone móvel.

Segundo Heary (2010), após a introdução do *Chip Card* este tipo de golpe diminuiu muito devido à utilização de criptografia na transmissão das informações.

A Figura 4.2 ilustra o exemplo de um equipamento ATM com *Skimming* instalado.

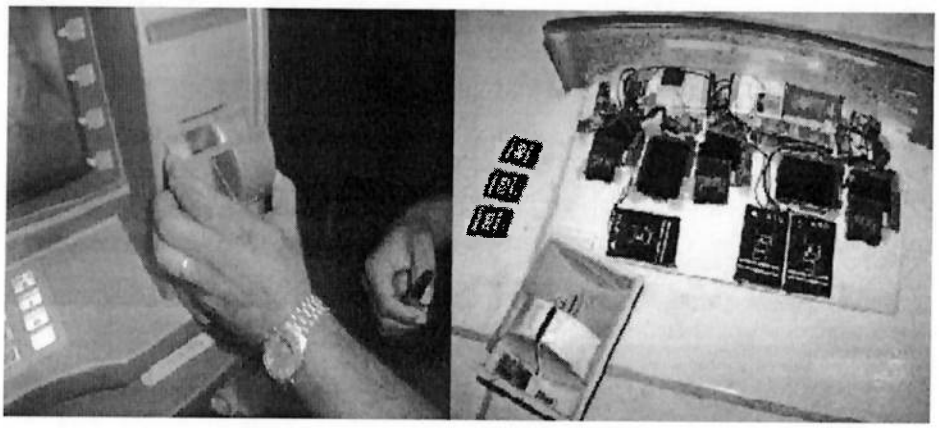


Figura 4.2 – ATM com *Skimming*

3.7 Ameaça por captura WEB

De acordo com Centro de estudos, respostas e tratamento de incidentes de segurança no Brasil (2010), as fraudes na internet têm utilizado amplamente *e-mails* com discursos que, na maioria dos casos, envolvem engenharia social e que tentam persuadir o usuário a fornecer seus dados pessoais e financeiros. Em muitos casos, o usuário é induzido a instalar algum código malicioso ou acessar uma página fraudulenta, para que dados pessoais e sensíveis, como senhas bancárias e números de cartões de crédito, possam ser furtados.

O *phishing scam* é o termo originalmente criado para descrever o tipo de fraude que se dá através do envio de mensagem não solicitada, que se passa por comunicação de uma instituição conhecida, como um banco, empresa ou site popular, e que procura induzir o acesso a páginas fraudulentas, projetadas para furtar dados pessoais e financeiros de usuários.

A palavra *phishing* (de "*fishing*") vem de uma analogia criada pelos fraudadores, onde "iscas" (*e-mails*) são usadas para "pescar" senhas e dados financeiros de usuários da Internet.

Atualmente, este termo vem sendo utilizado também para se referir aos seguintes casos:

a) Mensagem que procura induzir o usuário à instalação de códigos maliciosos, preparados para furtar dados pessoais e financeiros;
b) Mensagem que, no próprio conteúdo, apresenta formulários para o preenchimento e envio de dados pessoais e financeiros de usuários.

A Figura 4.3 ilustra uma imagem ironizando uma atividade *Phishing*.

Figura 4.3 - Phishing

De acordo com Sambray, McClure e Kurtz (2002), um dos ataques mais efetivos para captura de informações é conhecido como "Ataque de *e-mail* seguro para execução de *scripts*". Neste caso não é necessário que a vítima realize alguma interação com o *e-mail* recebido, basta apenas ler a mensagem ou selecionar através do painel de visualização da ferramenta de leitura de *e-mail*, pois o código é executado através do controle *ActiveX* do sistema Operacional. Sambray, McClure e Kurtz (2002) ainda destacam que é importante declarar a sintaxe MIME (*Mult-Part Internet Mail Extensions*) de forma que a mensagem seja formatada corretamente. O código abaixo ilustra um exemplo de ataque de *e-mail* seguro com o objetivo de criar um arquivo de *script* no diretório de inicialização sistema.

```
helo            algumdominio.com
mail from:      <atacante@mal-intencionado.net>
rcpt to:        <vitima@indefesa.net>
data
subject:        Leia isto sem falta!
MIME-Version:       1.0
Content-Type:text/html;     charset=us=ascii
Content-Transfer-Encoding:  7bit
Se esta mensagem foi recebida por engano, exclua-a imediatamente.
<object id = "scr" classid=clsid:06290BD5-48AA-11D2-8432-006008C3FBFC">
</object>
```

```
<SCRIPT>
scr.Reset();
src.Path="C:\\windows\\Menu Iniciar\\Programas\\Iniciar\\script.hta";
scr.Doc="<object id='wsh' classid='clsid:F935DC22-1CF0-11D0-ADB9-
00C04FD58A0B'></object><SCRIPT>wsh.Run('c:\\command.com');</"+"SCRIPT>";
scr.write();
</SCRIPT>
</object>
```

3.8 Ameaça por captura TEF e POS (PDV)

De acordo com Amorim (2001), quadrilhas especializadas em clonagem de cartões através de equipamentos POS ou TEF utilizam técnicas de "*Skimming*" ou golpe do chupa-cabras para roubar e armazenar dados de cartão de crédito. Esta técnica é semelhante à abordagem aplicada a dispositivos ATM, entretanto para este caso, os alvos são comércios de pequeno e médio porte como postos de combustíveis, cafés, supermercados, lojas de *shoppings centers* entre outros.

O golpe basicamente inicia quando um integrante da quadrilha se passa por um colaborador da companhia de cartão de crédito, que em visita ao estabelecimento alvo, substitui o equipamento normal por outro preparado para interceptar as informações das transações. Este equipamento fica no estabelecimento pelo período máximo de quinze dias e é novamente substituído, da mesma maneira que foi retirado, por outro normal "não preparado".

De posse do equipamento preparado com as informações, o fraudador descarrega os dados capturados em um sistema computacional com impressora de confecção de cartões, preparada para emitir novos cartões idênticos aos originais.

Os equipamentos preparados para interceptação de transações são montados com circuitos elaborados com alta tecnologia e grande capacidade de armazenamento. A figura 4.4 ilustra alguns equipamentos que foram apreendidos pela polícia e que estavam sendo utilizados para realização de clonagem de cartões, onde (à esquerda) um sistema computacional com impressora, e (à direita) um equipamento POS preparado para interceptação de transações.

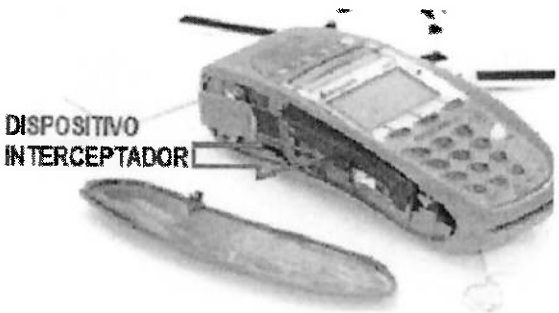


Figura 4.4 – Sistema de clonagem de cartões e interceptação de dados.

3.9 Ameaça por captura Telefone

De acordo com a Cielo (2010), quando há indisponibilidade dos sistemas de PDV (POS) e TEF nos estabelecimentos comerciais, o lojista pode optar pela transação por telefone ou TEF discado. Apesar de ser um meio de comunicação extremamente seguro, este tipo de transação consiste na ligação telefônica para central de cartões onde um sistema baseado em Unidade de Resposta Audível (URA) auxilia o comerciante com a entrada e transmissão dos dados do cartão.

Utilizando técnicas de "grampo telefônico", fraudadores podem interceptar estas informações, descriptografar os dados e realizar a clonagem de cartões utilizando como base os princípios já apresentados neste trabalho.

Existem diversas técnicas para realização do grampo telefônico, entretanto de acordo com Braga (2008), a forma mais segura e mais utilizada de interceptação de conversas telefônicas consiste na conexão da linha a um transmissor que envia seus sinais para um local seguro, onde o fraudador, com a ajuda de um receptor conectado a um gravador, armazena as conversas e dados transmitidos. A Figura 4.5 ilustra um esquema de interceptação telefônica a través do grampo.

Figura 4.5 – Esquema simples de grampo telefônico

4.0 Autenticação em rede transacional

O presente capítulo aborda os modelos de autenticação por banda magnética e *Chip;* O atual modelo de autenticação e autorização de transações que esta em operação na maior parte das redes transacionais; Uma proposta para aumentar a segurança na autenticação e autorização de transações por cartão, com o objetivo de mitigar os riscos e as ameaças nos pontos onde ocorrem as fraudes; E a conclusão deste trabalho.

4.1 Autenticação por Banda Magnética e *Chip*

De acordo com Monitor de Fraudes (2009), o desenvolvimento dos cartões de crédito com *Chip*, ou "*smart cards*" é considerada como a principal evolução na indústria mundial dos sistemas de pagamento.

Atualmente o principal sistema de armazenagem de dados nos cartões de crédito ainda é o de Banda Magnética. Esta tecnologia é considerada inadequada, devido às necessidades de segurança do setor. Esta modalidade de autenticação ainda existe para manter a compatibilidade entre sistemas e países onde o *Chip* ainda não foi introduzido.

As principais limitações da Banda Magnética são a inexistência de proteção por criptografia, capacidade de armazenamento limitada e facilidade de reprodução e clonagem.

Cartões que utilizam o sistema de *Chip* têm a capacidade de armazenar dados de forma segura (criptografados assimetricamente), maior capacidade de memória e um sistema de microprocessador interno que pode ser utilizado por múltiplas funções, sendo que no mesmo cartão podem ser armazenados dados de vários serviços diferentes. Outra vantagem importante é que até o momento não existe histórico de clonagem de *Chip*.

Entre os cartões com *Chip* se destaca o padrão EMV, criado a partir de 1993 pela colaboração das empresas de pagamento mundiais (*Europay*, *Mastercard* e *Visa*).

O padrão EMV define quatro elementos básicos de segurança nas aplicações financeiras dos cartões:

a) Autenticação do cartão off-line, ou seja, o terminal deve identificar o cartão como genuíno sem ter que se conectar com a rede transacional.

b) Parâmetros de gestão do risco. O cartão grava todas as transações e emite um alarme caso haja irregularidades.

c) PIN *off-line* - Os cartões com *Chip* podem armazenar dados de forma segura e sigilosa, permitindo que a verificação do PIN (Número de Identificação Pessoal ou senha do cartão) possa ser feita internamente sem a necessidade de se conectar a rede transacional.

d) Autenticação *on-line* - Se necessário ou casualmente, pode ser realizada a validação *on-line* do cartão através de conexão com a rede transacional.

As principais diferenças entre os cartões com *Chip* e os de Banda Magnética são:

Cartões com Banda Magnética utilizam o sistema CVV (*Card Verification Value*) que são os três dígitos na parte de traz do cartão. Este recurso somente pode ser utilizado para transações *on-line*.

Cartões com *Chip* utilizam diferentes técnica que permitem a autenticação seja *on-line* ou *off-line*:

SDA (*Static Data Authentication*) - É a tecnologia mais simples e de menor custo. Esta técnica permite que o cartão seja identificado e autenticado pelo terminal, através do uso dos dados e a assinatura digital contidos no *Chip*.

DDA (*Dynamic Data Authentication*) - Esta técnica permite que o sistema crie uma assinatura digital diferente para cada operação *off-line*. Esta tecnologia é mais segura, entretanto seu custo é aproximadamente 25% maior que a SDA.

CDA (*Combined Dynamic and Data Authentication*) - O cartão gera um "*Application Cryptogram*" e uma assinatura digital. O terminal verifica a assinatura digital, e determina se o *Application Cryptogram* foi gerado por um cartão genuíno.

Objetivos do *Chip*:

a) Redução de fraudes, falsificações e clonagens de cartões;

b) Aumentar o número de transações. Os sistemas de pagamento atuais necessitam de uma conexão *on-line* para realizar a autenticação, o que resulta na necessidade de maior tempo e custo por cada transação. *Smart cards* podem ser autenticados sem conexão, proporcionando agilidade nas transações por cartão;

c) Maior interoperabilidade entre bancos e sistemas de pagamento, seja no contexto nacional ou internacional;

d) Definição de um único padrão para os cartões de crédito, eliminando a necessidade de diferentes terminais para diferentes bandeiras;

e) Possibilidade de desenvolvimento de aplicações seguras para o comércio e pagamentos via internet.

Vale ressaltar que cartões com *Chip* dispensam a assinatura no verso do cartão, pois todas as transações são baseadas no código PIN.

4.2 Modelo atual de autenticação e autorização transacional

Atualmente a autenticação e a autorização transacional de cartão de crédito ocorrem de modo linear, ou seja, os dados utilizam o mesmo meio de comunicação para entrada, processamento e saída de dados, sendo que a entrada e a saída ocorrem no estabelecimento credenciado. A parte interativa desta atividade se resume somente aos dados do cartão que passam pelo processo de leitura no dispositivo de captura e a senha digitada, que é de conhecimento do proprietário do cartão. A transação basicamente ocorre da seguinte maneira: (Por motivo de segurança, a fonte das informações não pode ser divulgada).

a) A transação inicia no estabelecimento credenciado (ponto de captura) onde os dados do cartão e a senha são enviados para rede de captura;

b) Os dados do cartão são recebidos na rede de captura e passam pelo processo de checagem de consistência incluindo a senha do proprietário. Caso os dados estejam corretos, a mensagem é enviada para rede adquirente onde é adicionada de um *ticket* de aceite que é denominado de "*ticket* de bilhetagem". Caso os dados não estejam corretos, a transação é finalizada e o sistema envia ao ponto de captura a mensagem de transação rejeitada com o código definido pela bandeira;

c) Na rede adquirente, a mensagem é submetida aos sistemas de análise de fraude, inadimplência e bloqueio. Caso as informações estejam dentro dos padrões estabelecidos, a mensagem recebe o *ticket* de bilhetagem é enviada para rede da bandeira. Caso as informações não cumpram os padrões estabelecidos, as informações são processadas, armazenada, a transação é finalizada e o sistema envia ao ponto de captura a mensagem de transação rejeitada com o código definido pela bandeira;

d) Em seguida, a mensagem é recebida na rede da bandeira, onde é realizada a checagem da origem do cartão. Caso a transação seja proveniente de um cartão de outro país, a mensagem é enviada para a sede do cartão onde é realizado o processamento de acordo com os padrões de cartão internacional estabelecido pela bandeira. Ao seu retorno, a mensagem é enviada para a rede adquirente, caso a transação esteja aprovada a mensagem recebe a bilhetagem, caso contrário a bilhetagem não ocorre. Para transações da mesma praça, a mensagem recebe a bilhetagem e em seguida é entregue para a rede bancária;

e) Após o recebimento da mensagem na rede bancária, a análise de crédito é realizada. Nesta fase do processamento, o banco analisa o perfil do cliente com relação ao valor da transação que esta sendo realizada. Caso a transação seja aprovada, a mensagem recebe a bilhetagem e é devolvida para a rede adquirente, caso contrário a mensagem é enviada para a rede adquirente com o código de operação recusada e não recebe a bilhetagem;

f) No retorno das demais redes para a rede adquirente, a mensagem é processada e armazenada. Caso a transação esteja aprovada, uma nova mensagem é gerada para o ponto de captura, informando que a transação foi aprovada, caso contrário uma mensagem é enviada informando que a transação foi recusada contendo o código definido pela bandeira.

A Figura 5.2 ilustra o fluxo de autenticação e autorização em modo linear que atualmente esta operação em uma rede transacional. (Por motivo de segurança, a fonte das informações não pode ser divulgada).

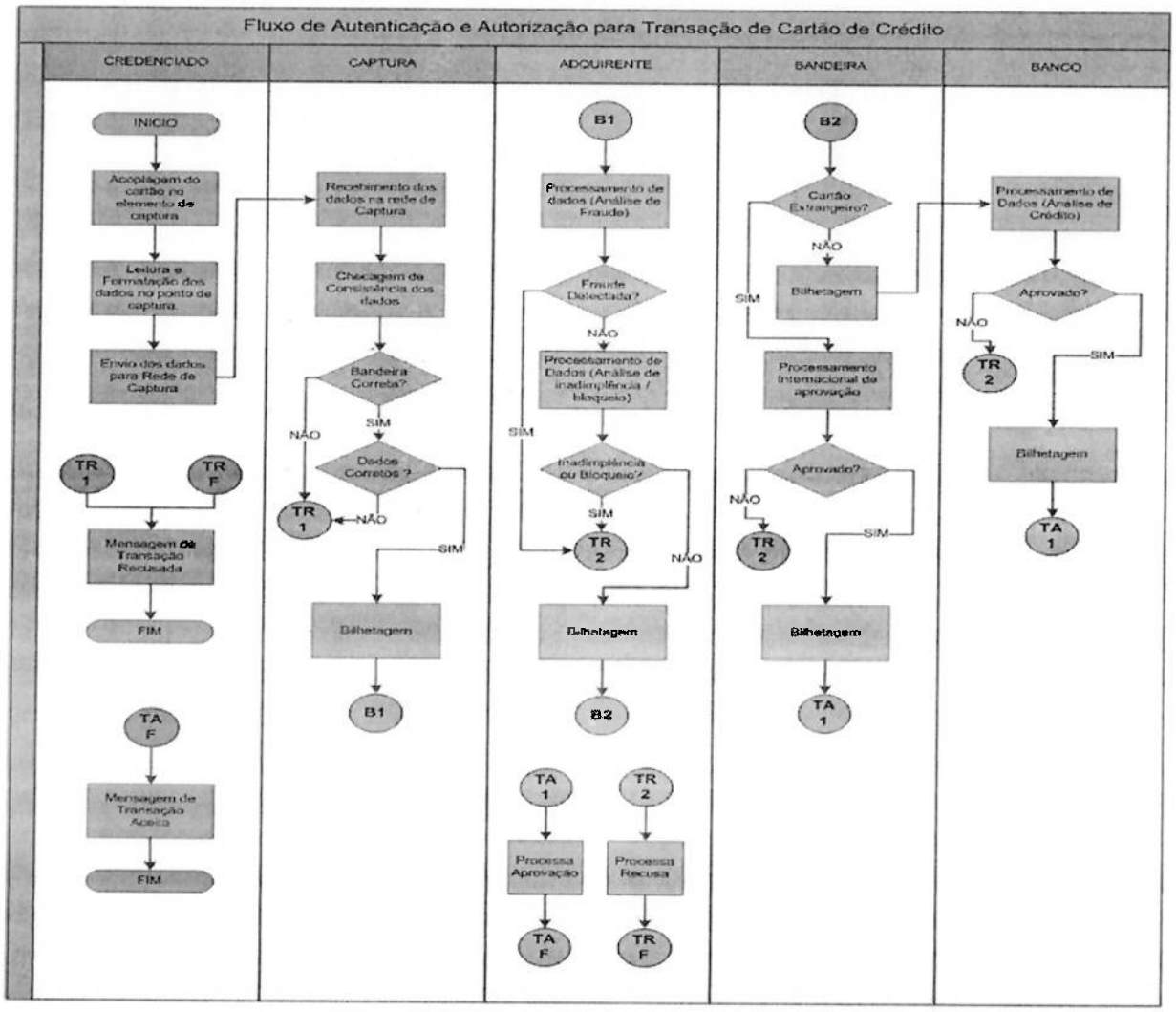


Figura 5.2 – Fluxo de autenticação e autorização transacional de cartão de crédito

4.3 Modelo proposto de autenticação e autorização transacional

Tomando como base o capítulo quatro do presente estudo, a principal ameaça de uma rede transacional de cartão de crédito esta relacionada à interceptação das informações do cartão e a senha (PIN) do proprietário ou portador. Também pode ser considerado que o ponto mais vulnerável do sistema, esta relacionado ao perímetro ou ponto de captura. Ainda de acordo com o capítulo quatro, as fraudes neste setor ocorrem principalmente por falhas de segurança no momento da captura e autenticação.

Com base nestas informações, pode ser constatada a necessidade de fortalecer o atual modelo linear de autenticação e autorização. A proposta deste estudo esta dirigida a propor um sistema de autenticação baseado em dupla custódia, ou seja, a primeira parte da senha deve ser de posse do proprietário do cartão (modelo atual de PIN), a segunda parte deve ser designada pela operadora de cartão no momento da captura e autorização.

Basicamente esta modalidade de autenticação é bem simples, ou seja, utilizando o atual sistema linear de autenticação, pode ser incluído um desvio no momento em que as informações entram na rede adquirente. Neste instante, o sistema deve gerar um código semelhante ao atual PIN, contendo de quatro a seis dígitos, por exemplo.

Este código deve ser enviado ou estar sincronizado com outro dispositivo em poder do cliente ou portador (pode ser utilizado como exemplo, dispositivos de *token* ou de telefonia móvel), informando também o valor da transação que esta sendo realizada. Após o recebimento da nova senha, o cliente deve digitar os números no ponto de captura. Neste momento a aplicação de controle da transação passa a aguardar a confirmação do código gerado, enquanto a transação continua com as demais etapas de checagem. Antes da conclusão da transação, o sistema de controle deve checar se a segunda senha confere com a senha digitada no ponto de captura.

No modelo de autenticação e autorização linear, a rede de captura centraliza toda a captação e transporte de dados. Neste modelo, a informação trafega por toda a rede transacional, sendo que em cada ponto de autorização a mensagem recebe a bilhetagem. Ao final, os dados são checados e devolvidos ao ponto de captura com a mensagem "transação autorizada". A Figura 5.3.1 ilustra o modelo de autenticação e autorização linear.

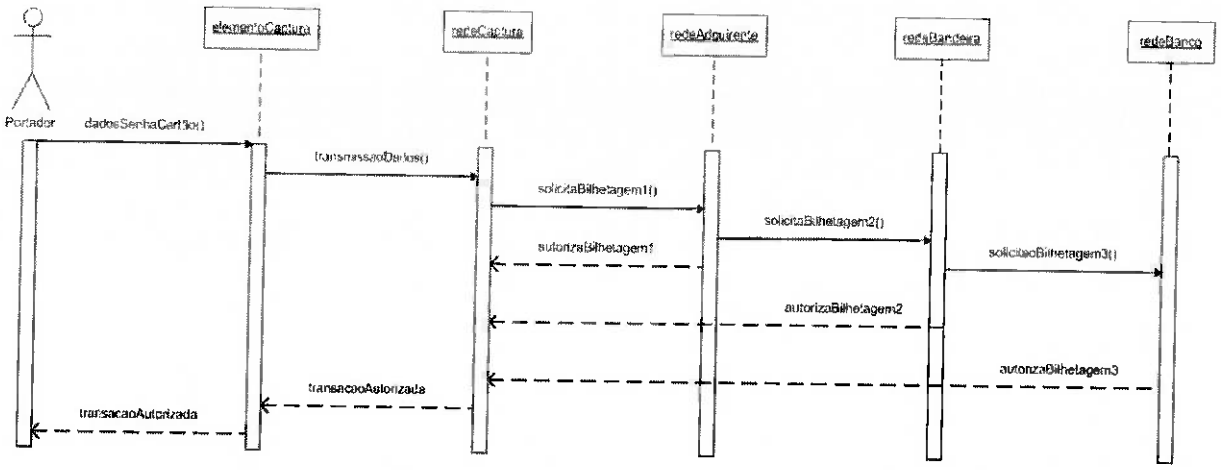
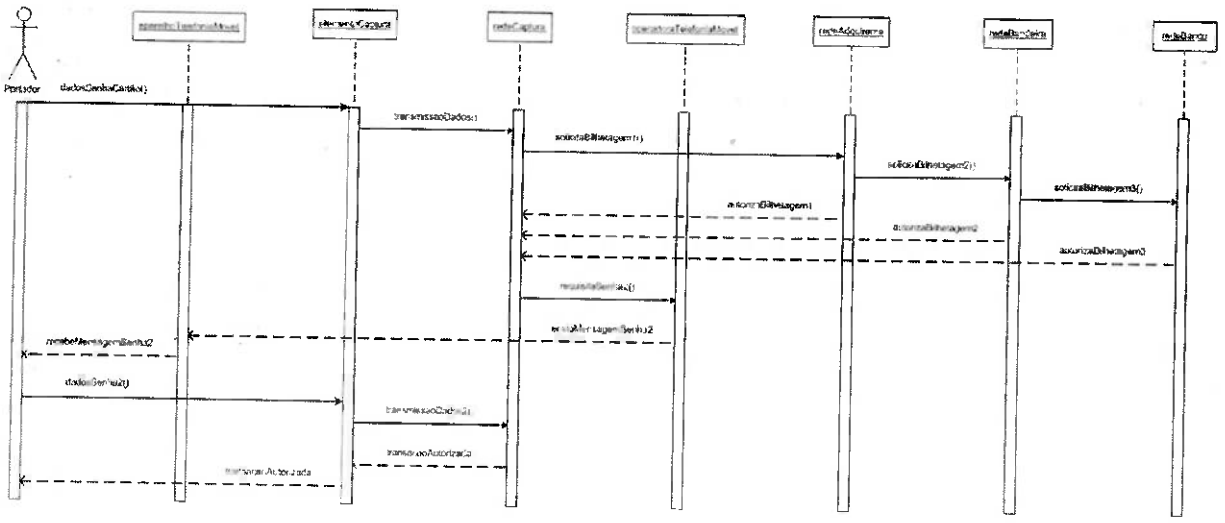


Figura 5.3.1 – Modelo de autenticação e autorização linear

No modelo de autenticação e autorização com dupla custódia, a informação segue o mesmo fluxo do modelo linear, entretanto de acordo com Burton, Chuvakin, Elberg, Freedman, King, Paladino e Shcooping (2007), os padrões PCI sugerem a autenticação de fator duplo. Neste modelo pode incluída uma operadora e aparelho de telefonia móvel, para realização do transporte e entrega da segunda senha, através da rede sem fio. A Figura 5.3.2 ilustra o modelo de autenticação e autorização com dupla custódia.



. Figura 5.3.2 – Modelo de autenticação e autorização com dupla custódia

Os pontos fortes para o modelo de autenticação e autorização com dupla custódia e segunda senha enviada para aparelho de telefonia móvel são:

a) Em caso de clonagem do cartão, no momento que o fraudador tentar realizar alguma transação, uma senha com o valor da transação será enviada ao

proprietário do cartão. O proprietário por sua vez, poderá imediatamente entrar em contato com a operadora de cartão e cancelar o produto;

b) Os aparelhos mais modernos de telefonia móvel possuem em seu sistema operacional, opções de segurança que incluem bloqueio por senha, ou seja, em caso de roubo do cartão, senha do cartão e aparelho de telefonia móvel, o meliante necessitará também a senha de acesso ao aparelho o que aumenta a dificuldade da ação dos marginais.

Os Pontos fracos para o modelo de autenticação e autorização com dupla custódia e segunda senha enviada para aparelho de telefonia móvel são:

a) O sistema de telefonia móvel não foi desenvolvido para enviar e receber *e-mails* com a agilidade esperada pelas transações de cartão. Lentidão nos sistemas de *e-mail* das operadoras de telefonia móvel pode impactar a operadora de cartões, devido à espera no recebimento da mensagem e que por conseqüência pode impactar os estabelecimentos gerando filas nos caixas. Outro ponto importante nesta modalidade é que os *e-mails* enviados pelas operadoras de cartão tendem a sofrer concorrência com mensagens normais que atualmente são transportadas por este sistema;

b) Esta modalidade de autenticação inviabiliza transações *off-line*, pois o modelo apresentado de autenticação por dupla custódia necessita que a segunda senha seja enviada no momento da transação.

Para solucionar os pontos fracos abordados, uma nova modalidade de autenticação está sendo ilustrada abaixo, utilizando um modelo híbrido de autenticação baseado em telefonia móvel e criptografia simétrica.

Em um modelo de autenticação de dois fatores, podem ser consideradas a inclusão de telefonia móvel e *tokens*, entre outros, para informar ao usuário qual senha deve ser utilizada no momento da transação, incluindo o PIN que é de seu conhecimento.

De acordo com Dandash, Wang, Dung e Srinivasan (2007) o protocolo KSL pode fornecer segurança para este tipo de comunicação, minimizando interceptações de comunicações em redes sem fio.

No caso da utilização de token, a abordagem do capítulo 3.3 (criptografia simétrica), as duas partes devem possuir copias dos certificados que estão em uso, ou seja, o cartão e o servidor devem possuir o mesmo certificado para realizar a geração da senha que deve ser enviada para o visor digital no cartão de crédito do portador.

De acordo com Konheim (2007), uma vez que a senha informada no visor digital e o PIN são digitados no elemento de captura, os dados devem ser enviados (seguindo o processo normal), para a rede de captura, onde o servidor de checagem de autenticação deve possui o mesmo código gerado no cartão de crédito. Conforme já

foi citado, este código deve ter validade de um minuto e deve estar em sincronia de horário tanto o cartão de crédito do portador quanto o servidor de autenticação.

Atualmente a indústria da tecnologia em seu segmento de segurança da informação, oferece produtos que executam esta função para VPN "*Client-toSite*", entretanto por motivos óbvios o nome do produto e o nome de seu respectivo fabricante, não são citados neste trabalho.

Para agregar segurança a esta modalidade transação, a rede de captura, após a realização da autorização, pode (por exemplo) enviar ao portador uma mensagem de *e-mail* através de sistema de telefonia móvel, informando os dados da transação. Esta mensagem deve ser recebida pelo portador que deve confirmar a transação dentro de um tempo mínimo a ser estimado. Neste caso, esta mensagem pode ser recebida posteriormente a transação, eliminando assim os problemas abordados em relação a transações *off-line*. Este tipo de modelo esta aderente aos estudos de Dandash, Wang, Dung e Srinivasan (2007).

Como a mensagem pode ser recebida posteriormente, isto dá ao usuário a possibilidade de cancelar uma transação indevida. Neste caso o cartão passa a ser cancelado imediatamente, impossibilitando ao fraudador realizar novas transações.

A Figura 5.3.4 ilustra um modelo de mensagem de aprovação de transação para cartão de crédito, simulando o envio das informações sobre a transação ao elemento de telefonia móvel. Na ilustração pode ser observado o questionamento sobre a aceitação da transação e a informação de cancelamento de cartão em caso de desaprovação.

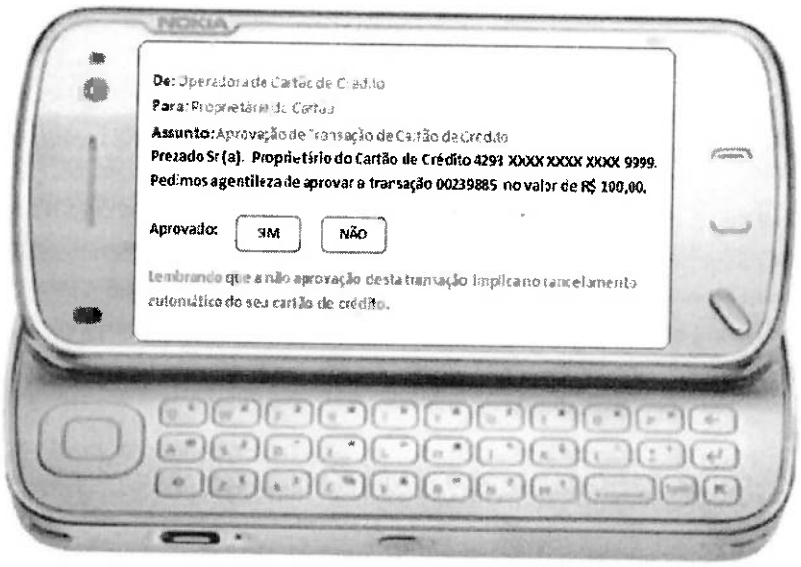


Figura 5.3.3 – Modelo de mensagem de aprovação de transação

Considerando as definições de padrão exigidas pela ISO-8530 um ponto fraco para este tipo de implantação pode ser a adaptação de hardware ao atual modelo de cartão magnético.

5.0 Conclusão

5.1 Considerações Finais

Este trabalho teve como missão, a pesquisa do modelo transacional de cartões de crédito, ilustrando em seu inicio os agentes relacionados à operação de autorização e liquidação e os canais de distribuição do cartão de crédito.

As pesquisas realizadas ao longo do presente trabalho tiveram o intuito de apresentar as informações em um formato simplificado para análise e entendimento dos padrões em relação aos modelos de prevenção a fraude e segurança de um ambiente transacional, onde foram ilustrados os principais controles de fraudes, tais como os sistemas baseados em inteligência artificial, análise de base de dados, criptografia e as normatizações baseadas em ISO e PCI-DSS que fortalecem a segurança interna e de perímetro.

Para melhor entendimento da questão e enriquecimento da pesquisa em relação ao tema, foram elencadas as ameaças e vulnerabilidades (relacionadas aos pontos de captura), que podem comprometer a segurança em um ambiente transacional.

O estudo de caso ilustrou os modelos de autenticação e autorização existentes, incluindo uma proposta baseada em dupla autenticação, para mitigar as fraudes relacionadas ao setor.

De acordo com este estudo, podemos concluir que com a integração da autenticação de dupla custódia (conforme proposta apresentada no capítulo 5), métodos alternativos para enrijecer a captura de transações podem mitigar ou eliminar as ameaças e vulnerabilidades de sistemas transacionais, tanto para fraude como para roubo e furto de cartões.

5.2 Trabalhos Futuros

A sugestão de continuidade deste estudo deve tratar da criação de um ambiente operacional e funcional para simular uma rede transacional com integração a sistemas de telefonia móvel e *token* incluindo os elementos de captura aqui mencionados. Para complementar, se faz necessário a adaptação de sistemas para recepção e autorização de informações, realizando a autenticação de dupla custódia e hardware compatível para adaptação de *token* com senha assimétrica.

REFERÊNCIAS

ABRAHAM, A.; GROSAN, C.; RAMOS, V. **Swarm intelligence in data mining.** Romênia: Springer, 2006.

AMORIM, P. H. Saiba como funcionava o esquema da quadrilha que clonava cartões em SP. **Rede Record de Televisão**, 18 abr. 2007. Disponível em: <http://noticias.r7.com/sao-paulo/noticias/saiba-como-funcionava-o-esquema-da-quadriilha-que-clonava-cartoes-em-sp-20100418.html>. Acesso em: dez. 2010.

ASSOCIAÇÃO BRASILEIRA DAS EMPRESAS DE CARTÕES DE CRÉDITO E SERVIÇOS. **A história do cartão de crédito,** [199?]. Disponível em: <http://www.abecs.org.br/quemsomos_historia.asp>. Acesso em: nov. 2010.

CENTRO DE ESTUDOS, RESPOSTAS E TRATAMENTO DE INCIDENTES DE SEGURANÇA NO BRASIL. **Cartilha de segurança para internet,** 2010. Disponível em: <http://cartilha.cert.br/fraudes/sec2.html>. Acesso em: dez. 2010.

BANCO CENTRAL DO BRASIL. **Diagnostico do Sistema de Pagamentos de Varejo no Brasil**, 2010. Disponível em: <http://www4.bcb.gov.br/?SPBVAREJO>. Acesso em: nov. 2010.

BRAGA, A.; CARVALHO, A.; LUDEMIR, T. **Redes neurais artificiais - teoria e aplicações.** Rio de Janeiro: LTC, 2000.

BRAGA, N. C. Grampo telefônico - entenda o que é e como evitar. **Saber Eletrônica**, 23 out. 2008. Disponível em: <http://www.sabereletronica.com.br/secoes/leitura/1017>. Acesso em: dez. 2010.

BURTON, J.; CHUVAKIN, A.; ELBERG, A.; FREEDMAN, B.; KING, D.; PALADINO, S.; SHCOOPING, P. **Understand and implement effective PCI data security standard compliance.** Burlington: Syngress, 2007.

CHAN, P. K.; FAN, W.; PRODROMIDIS, A. L.; STOLFO, S. J. Distributed data mining in credit card fraud detection. In: INTELLIGENT SYSTEMS AND THEIR APPLICATIONS, nov-dec. 1999. **[Computer Society]**. Miami: IEEE, ago. 2002. .p. 67.

CIELO. **Soluções de tecnologia,** 2010. Disponível em: <http://www.cielo.com.br/portal/cielo/solucoes-de-tecnologia.html>. Acesso em: nov. 2010.

DANDASH, Y.; WANG, Y.; DUNG, P.; SRINIVASAN, B. A new Dynamic Key Generation Scheme for Fraudulent Internet Payment Prevention. In: FOURTH INTERNATIONAL CONFERENCE ON INFORMATION TECHNOLOGY, 2-4 Apr. 2007. **[Proceedings]**. Las Vegas: IEEE, 2007. .p. 83-89.

DELFS, H.; KNEBL, H. **Introduction to cryptography - principles and applications.** Berlin: Springer, 2007.

FAWCETT, T.; PROVOST, F. Adaptive fraud eetection. In: DATA MINING AND KNOWLEDGE DISCOVERY, mar. 1997. **[Journal]**. Hingham: ACM, ago. 1997.

HIPERCARD. **Meios de captura,** [20-?]. Disponível em: <http://www.hipercard.com.br/pj/meios_de_captura/pos.asp>. Acesso em: nov. 2010.

JORNAL NACIONAL. Clonagem de cartões no Brasil aumenta quase 50%. **Globo ponto com**. 06 ago. 2009. Disponível em: <http://jornalnacional.globo.com/Telejornais/JN/0,,MUL1257829-10406,00-CLONAGEM+DE+CARTOES+NO+BRASIL+AUMENTA+QUASE.html>. Acesso em: out. 2010.

HEARY, J. Newest attack on your credit card pin pad shims. **Network World**, 07 nov. 2010. Disponível em: <http://www.networkworld.com/community/blog/newest-attack-your-credit-card-shims>. Acesso em: dez. 2010.

INTERNATIONAL ORGANIZATION FOR STANDARTIZATION. **Identification cards physical characteristics**, 2003. Disponível em: <http://www.iso.org/>. Acesso em: nov. 2010.

KONHEIM, A. **Computer security and cryptography.** New Jersey: John Wiley & Sons, 2007.

MA, H.; LI, X. Application of data mining in preventing credit card fraud. In: INTERNATIONAL CONFERENCE ON MANAGEMENT AND SERVICE SCIENCE, 20-22 Sep. 2009. **[Proceedings]**. Wuhan: IEEE, 2009. .p. 1-6.

MASTER CARD. **How MasterCard works**: understanding the transaction process and how you fit in, [20-?]. Disponível em: <http://www.mastercard.com/au/merchant/en/how_works/index.html>. Acesso em: feb. 2011.

MICROSOFT TECHNET, **Aprimorando a segurança de dados por meio do SQL Server 2005**, 01 out. 2005. Disponível em: <http://technet.microsoft.com/pt-br/library/bb735261.aspx>.

MONITOR DE FRAUDES. **Cartões com chip e o padrão EMV**, 19 fev. 2009. Disponível em: <http://www.fraudes.org/showpage1.asp?pg=109>. Acesso em: dez. 2010.

PEJIC-BACH, M. Profiling intelligent systems applications in fraud detection and prevention: survey of research articles. In: INTERNATIONAL CONFERENCE ON INTELLIGENT SYSTEMS, MODELLING AND SIMULATION, 2010. **[Proceedings]**. Piscataway: IEEE, 2010. .p. 80-85.

RIBEIRO, E. Fraudes em compras online causam temor em paulistanos. **ComputerWorld**, 04 ago. 2009. Disponível em: <http://computerworld.uol.com.br/seguranca/2009/08/04/fraude-em-compras-online-causam-temor-em-paulistanos/>. Acesso em: out. 2010.

RICHARDSON, R. Neural networks compared to statistical techniques. In: COMPUTATIONA INTELLIGENCE FOR FINANCIAL ENGINEERING, 23-25 mar. 1997. **[Proceedings]**. New York City: IEEE, ago. 2002. .p. 89-95.

RUSSO, B. Especialista comenta cuidados para transações com cartões de crédito. **Modulo Security,** [200?]. Disponível em: <http://www.modulo.com.br/sala-de-imprensa/182-1107-especialista-comenta-cuidados-para-transacoes-com-cartoes-de-credito >. Acesso em: out. 2010.

SAMBRAY, S; MCCLURE, S.; KURTZ, S. **Hackers expostos - segredos e soluções para a segurança de redes.** 2. ed. São Paulo: Makron Books, 2002.

SANTOS, R. A. F. Uso de Redes neurais artificiais na detecção de fraudes. **Serasa Experian**, 2011. Disponível em: <http://www.serasaexperian.com.br/serasaexperian/publicacoes/revista/2007/63/revista_0341.htm>. Acesso em: Nov. 2010.

SUPORTE MICROSOFT. **Descrição da criptografia simétrica e assimétrica**, 26 out. 2007. Disponível em: <http://support.microsoft.com/kb/246071/pt-br/>. Acesso em: dez. 2010.

VAMOSI, R. Saiba como se proteger contra a clonagem do cartão de crédito. **IDG Now**, 10 dez. 2010. Disponível em: <http://idgnow.uol.com.br/seguranca/2010/12/10/saiba-como-se-proteger-contra-a-clonagem-do-cartao-de-credito/>. Acesso em: dez. 2010.

GLOSSÁRIO

ActiveX	Conjunto de tecnologias criado para facilitar a integração entre diversas aplicações.
Adquirente	Empresa responsável pelo credenciamento, gerenciamento e relacionamento entre as bandeiras de crédito e débito e os estabelecimentos comerciais.
Autorização	Pedido feito pelo estabelecimento onde está sendo realizada a compra à administradora do cartão. São enviados o número do cartão, o valor da compra e a validade do mesmo. A resposta é dada pelo terminal eletrônico (POS ou PDV).
Bandeira	Marca do cartão. A bandeira define as regras do cartão. As bandeiras precisam se associar aos emissores (bancos) de cartões para que o financiamento do cartão aconteça.
Capturar	Realizar uma venda com cartão de crédito ou débito, por meio e um terminal eletrônico (POS ou PDV) no estabelecimento, através de uma venda remota (site ou *call center*) ou por meio do celular.
Credenciado	Estabelecimento ou empresa que aceita determinado cartão de crédito.
Emissor	Administradora do cartão. Em geral são os bancos e as empresas prestadoras de serviços que emitem e gerenciam o cartão de crédito. O emissor é quem, de fato, financia o crédito do cartão e quem estabelece a taxa de juros e os limites de crédito.
Fatura	Demonstrativo de todas as transações (débitos e créditos) ocorridas e que justificam o valor a ser pago pelo portador do cartão. A fatura também informa limite de crédito, vencimento, valor para pagamento integral e pagamento mínimo, eventuais encargos, débitos de anuidades e taxas.
Phishing	Método de roubo de identidade efetuado através da criação de um site que parece representar uma empresa legítima. Os visitantes do site, pensando que estão comprando algo de um negócio real, apresentam as suas informações pessoais para o site. Os criminosos, em seguida, usam as informações pessoais para seus próprios fins.

POS/PDV	(*Point of Sale* / Ponto de Venda) São os terminais eletrônicos utilizados pelos estabelecimentos para pedir autorização, registrar operações feitas com cartão de crédito ou débito e para imprimir o comprovante de venda. A leitura da tarja magnética ou chip dos cartões faz a identificação e o envio do pedido de autorização automaticamente à administradora, que vai autorizar ou negar a transação.
Processadora	Empresa responsável pela parte operacional dos cartões, como o processamento de faturas e o atendimento ao cliente.
Skimming	Método eletrônico de captura de informações pessoais usado por ladrões de identidade. O *skimmer* é um pequeno dispositivo que digitaliza um cartão de crédito e armazena as informações contidas na fita magnética. O *Skimming* pode ocorrer durante uma transação de cartão de crédito ou débito.
Titular	Proprietário do cartão em casos em que há dependentes (cartões adicionais). É também o responsável contratual e juridicamente pelo cartão.
X.25	É um conjunto de protocolos padronizado pela ITU para redes de longa distância e que usam o sistema telefônico ou ISDN como meio de transmissão.