UNIVERSIDADE FEDERAL DE SANTA CATARINA
PROGRAMA DE PÓS-GRADUAÇÃO EM CIÊNCIA DA COMPUTAÇÃO

Luciana Rita Guedes Ghisleri

Um Protocolo Criptográfico para Auditoria de Publicidade na Web

Dissertação submetida à Universidade Federal de Santa Catarina como parte dos requisitos para a obtenção do grau de mestre em Ciência da Computação.

Prof. Ricardo Felipe Custódio, Dr.
Orientador

Florianópolis, Fevereiro de 2003

Um Protocolo Criptográfico para Auditoria de Publicidade na Web

Luciana Rita Guedes Ghisleri

Esta Dissertação foi julgada adequada para a obtenção do título de mestre em Ciência da Computação, área de concentração Sistemas de Computação e aprovada em sua forma final pelo Programa de Pós-Graduação em Ciência da Computação.

_____

Prof. Fernando Ostuni Gauthier, Dr.

Coordenador do Curso

Banca Examinadora

_____

Prof. Ricardo Felipe Custódio, Dr.

Orientador

_____

Prof. Carlos Alberto Maziero, Dr.

_____

Prof. Carlos Roberto De Rolt, Dr.

“Nesta era de conectividade eletrônica universal, de vírus e hackers, de espionagem e fraude eletrônica, não há momento em que a segurança não importe.”
Cryptography and Netword Security, William Stallings
(tradução pessoal)

Ofereço este trabalho a meu esposo, Amauri Sant’ Anna Ghisleri, companheiro de profissão e de vida, a quem amo e admiro mais a cada dia durante estes dez anos em que estamos casados.

Agradecimentos

Quero agradecer em primeiro lugar a meus pais, que além de me trazerem ao mundo, sempre se preocuparem em me garantir a educação, em todos os sentidos, e cujos esforços me fizeram chegar até aqui.

Agradeço também a meu esposo, melhor amigo e companheiro de todas as horas que, com seu olhar crítico, contribuiu com as revisões deste trabalho.

A meu orientador, excelente professor, a quem muito admiro como profissional e como pessoa.

Aos alunos de graduação da Universidade Federal de Santa Catarina, Fernando José Karl e Geovane Pasa, que trabalharam arduamente para implementar a protocolo proposto neste trabalho.

Ao amigo Wesley Masterson Belo de Abreu que, ao me apresentar ao prof. Custódio, abriu-me o caminho para iniciar este trabalho.

Minha gratidão também aos mestres e amigos, incontáveis colaboradores, que me ensinaram, incentivaram e ajudaram direta e indiretamente no decorrer desta caminhada.

Sumário

Lista de Figuras

Lista de Tabelas

Resumo

O objetivo deste trabalho é propor um protocolo criptográfico para auditoria de publicidade na Web.

Um dos problemas que este protocolo propõe-se a resolver é a questão da medição da efetividade de anúncios publicados na Internet, isto é, como saber quantos clientes fizeram suas compras motivados por um anúncio publicado em um determinado sítio da Web. Outro problema está relacionado à garantia de que o sítio contratado para publicar os anúncios em sua página da Internet esteja cumprindo o acordo em termos de freqüência e horário em que estes anúncios são publicados.

O protocolo visa garantir que estes problemas sejam resolvidos, tendo em vista especialmente as questões ligadas à segurança já que a Web constitui-se num meio de comunicação vulnerável sob este aspecto.

Técnicas de criptografia, assinatura digital, protocolização digital de documentos eletrônicos entre outras ferramentas que visam a segurança em transações na Web são utilizadas no protocolo aqui proposto.

Palavras-chave: medição de audiência, publicidade na Internet, protocolos criptográficos.

Abstract

The aim of this job is to propose a cryptographic protocol for advertising audit on the Web.

One of the problems this protocol solves is the matter of effectiveness of Web advertisements. That is, how to know the number of clients who did their purchasing persuaded by an ad published on a certain site of the Web. Another problem has to do with the warranty that the site you have hired to publish your advert on their pages will fulfil the terms concerning frequency and times of broadcasting.

The protocol aims at assuring that these problems are solved, as well as providing safety, in that the Web is a vulnerable means of communication regarding this aspect.

Cryptography techniques, digital signature, digital time stamping of electronic documents, among other tools which aim at safety in Web trades are used in the protocol herein proposed.

Keywords: Audience measurement, Advertising on the Web, Cryptographic protocols.

Capítulo 1

Introdução

A Internet é atualmente um meio de comunicação de importância incontestável. Como tal, constitui-se também num meio de publicidade com características muito peculiares. O principal diferencial da Internet sobre os demais meios de comunicação é a interatividade, isto é, a possibilidade do usuário em "dialogar", interagir.

Outro diferencial da Internet é que usuário faz seus próprios horários e não há um *"horário nobre"* comum a todos como acontece com outros meios como a televisão e o rádio [NEG 95]. No rádio e na televisão, as informações são difundidas (através de estações repetidoras, por exemplo) para todos os "espectadores" ao mesmo tempo. Ou seja, todos recebem a mesma informação (apenas com alguma variação conforme a região onde haja uma programação local em certos horários) simultaneamente. A característica da propagação simultânea da informação resulta na valorização de determinados horários nos quais pode-se observar uma maior quantidade de pessoas utilizando seus aparelhos receptores (esses horários, dito "nobres", são chamados de "picos de audiência").

Outra característica importante da Web[1] é o crescimento do número de usuários. A tabela 1.1 mostra a estimativa de usuários que têm acesso à Internet nas diversas regiões do mundo.

Uma pesquisa do Ibope realizada em dezembro de 2000 revelou que

[1] Segundo o dicionário Aurélio [FER 99] a palavra Web deriva do inglês e significa literalmente "teia"; seu uso na Informática corresponde à forma reduzida de "*Worldwide Web*" ou "teia (de âmbito) mundial"; esta palavra freqüentemente é utilizada para referenciar a própria Internet, como é o caso neste documento.

Tabela 1.1: Usuários Conectados à Internet no Mundo: Número de usuários em milhões.

Local	**Usuários**	**Percentual**
África	6,31	1,04%
América Latina	33,35	5,51%
Ásia/Pacífico	187,24	30,92%
Europa	190,91	31,52%
EUA & Canadá	182,67	30,16%
Oriente Médio	5,12	0,85%
Mundo Todo	**605,60**	**100,00%**

Fonte: NUA Internet Surveys - jan/2003[2]

"cerca de 15% dos internautas das nove principais regiões brasileiras fizeram compras pela Internet. Em números absolutos, isto representa quase um milhão de compradores online" [IBO 01]. Ainda segundo pesquisa mensal deste mesmo instituto, *"Em julho de 2002, o Brasil registrou crescimento de 2,9% no número de internautas ativos, atingindo 7,8 milhões de pessoas. O número de cidadãos com acesso à internet em residências continuou em 14 milhões.*". Considera-se usuário ativo aquele que acessa a Internet regularmente. É importante salientar que estes números englobam somente os usuários brasileiros, que representam apenas uma pequena parcela do total mundial. A figura 1.1 mostra esta evolução.

Segundo dados do Livro Verde publicado pelo Ministério da Ciência e Tecnologia (MCT) em 2000, o Brasil estava em 13^o lugar em número de *hosts*, o que representa aproximadamente 1% do total mundial [SDI 00], conforme mostra a tabela 1.2.

O comércio eletrônico, introduziu características inovadoras às transações comerciais, tanto para quem vende quanto para quem compra. Para os clientes, a comodidade de comprar sem se deslocar de sua casa ou escritório, além da facilidade de pesquisa de preços e da possibilidade de, em muitos casos, obter assistência técnica pela

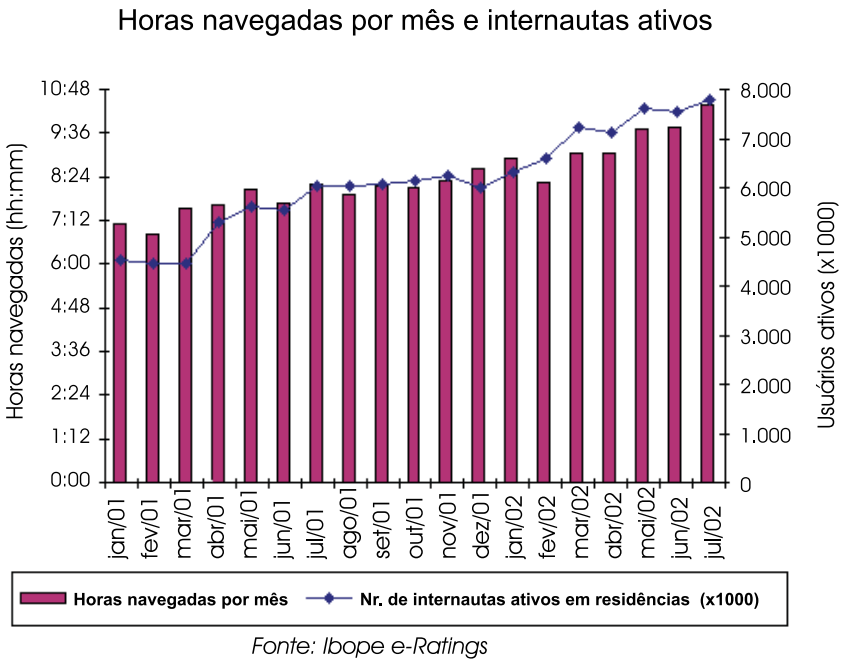


Figura 1.1: Evolução de usuários da Internet. A pesquisa Ibope realizada mensalmente mostra uma tendência contínua de crescimento tanto no número de usuários ativos (que acessam regularmente a Internet) quanto no tempo médio diário de horas em que eles ficam "conectados".

própria rede são algumas das vantagens. Para fornecedores, a ampliação de mercado a nível mundial e em tempo integral, além da redução de custos são atrativos para investir em comércio eletrônico. Mais ainda, *"A Internet torna-se também um meio muito eficiente de fazer publicidade direcionada ao mercado-alvo das empresas"*, conforme é citado no Livro Verde do MCT [SDI 00]. As características vantajosas do uso da Internet como meio de publicidade têm atraído em quantidade igualmente crescente o número de empresas que buscam este meio para anunciar seus produtos e serviços.

Entretanto, se por um lado é possível enumerar uma série de vantagens atrativas para o uso da Internet como meio de publicidade, por outro, existem dificuldades que ainda impedem algumas empresas de empregar a Internet para anunciar seus produtos/serviços.

Uma destas dificuldades é a questão sobre "onde" anunciar. Em geral,

Tabela 1.2: Classificação dos Países por Número de Hosts

Classificação	País	Número de Hosts
1º	Estados Unidos	53.167.229
2º	Japão	2.636.541
3º	Reino Unido	1.901.812
4º	Alemanha	1.702.486
5º	Canadá	1.669.664
6º	Austrália	1.090.468
7º	Holanda	820.944
8º	França	779.879
9º	Itália	658.307
10º	Finlândia	631.248
11º	Taiwan	597.036
12º	Suécia	594.627
13º	Brasil	446.444
14º	Espanha	415.641
15º	México	404.873

Fonte: SEPIN - MCT - Brasil - janeiro/2000 - em [dPdIeA 00].

empresas que usam a Internet como meio de publicidade constroem seus próprios sítios onde apresentam a própria empresa e seus produtos. O problema encontra-se em “como atrair os clientes potenciais para este sítio da empresa?”, “como fazer com que saibam da existência deste sítio e fazer com que o visitem?”. Uma opção para resolver o problema é o uso da técnica de “mix de mídia”, onde outros meios (televisão, rádio, outdoor) podem ser usados para tornar público o endereço da empresa no “mundo virtual”. Outra opção para as empresas está na escolha de sítios que publiquem seus anúncios. Neste caso, o desafio está em escolher sítios que tenham uma boa audiência e que atinjam o público-alvo desejado atraindo potenciais consumidores para o sítio da empresa. Uma alternativa

muito comum são os sítios dos motores de busca[3] que atualmente dispõem de técnicas avançadas e, além de apresentar ao usuário a lista de endereços relativos à sua pesquisa, podem também apresentar um anúncio de uma empresa que tenha relação com a palavra ou expressão pesquisada.

Mais uma dificuldade ligada ao uso da Internet como meio de publicidade diz respeito a garantir que um sítio contratado para publicar o anúncio o faça dentro das regras estabelecidas no referido contrato. Ou seja, após escolhido o(s) sítio(s) que irá veicular o anúncio da empresa, garantir que este(s) publique(m) o anúncio nos horários combinados e/ou com a freqüência pré-determinada. No caso de meios de publicidade como a televisão e o rádio existem sistemas de auditoria computadorizados que monitoram a programação continuamente e indicam precisamente se a quantidade de inserções[4] foram aquelas combinadas em contrato e até mesmo se um comercial foi veiculado na íntegra, isto é, se não houve interrupção ou falha na apresentação.

Outra grande dificuldade encontrada no uso da Internet para anunciar produtos/serviços constitui-se em medir o sucesso deste tipo de publicidade. A questão neste caso é como obter, com a maior precisão possível, o retorno alcançado pelos anúncios. Em outras palavras, como descobrir o quanto o anúncio contribuiu efetivamente no aumento do volume de vendas ou contratos ou mesmo simplesmente quantas pessoas tiveram acesso ao anúncio.

No caso da "publicidade convencional"[5] existem diversos institutos especializados em promover informações de aferição de audiência através do emprego de metodologias apropriadas. Entre os mais conhecidos[6] estão o Ibope, os Estudos Marplan

[3]Os sítios de motores de busca ou sítios de busca são amplamente utilizados pelos internautas quando procuram informações na Internet; com eles o usuário pode obter uma lista de endereços eletrônicos de seu interesse digitando uma palavra ou expressão.

[4]O termo inserção é usado na área de Propaganda e Publicidade para indicar cada "aparição" de um comercial num meio de comunicação como rádio ou tv.

[5]A expressão 'publicidade convencional' é aqui utilizada para indicar toda forma de publicidade que não seja pela Internet; seu emprego não condiz com a descrição formal da área de Publicidade e Propaganda.

[6]Os institutos aqui mencionados bem como as metodologias por eles utilizadas serão descritas com mais detalhes no capítulo 2.

e o IVC. As informações fornecidas por estas entidades oferecem meios para as empresas selecionarem suas estratégias de mídia. Entre outras decisões possíveis, uma empresa pode escolher anunciar em um determinado canal de TV, ou numa estação de rádio conforme os resultados apontados por aqueles institutos.

Para alguns destes problemas apresentados já existem algumas técnicas que visam resolvê-los como, por exemplo, a contagem por cliques e os cupons eletrônicos, como será discutido no capítulo 3. Porém, estas técnicas não garantem resultados precisos e, em alguns casos, podem permitir fraudes. Assim sendo, o ideal seria encontrar técnicas que garantam resultados seguros e precisos.

O LabSec (Laboratório de Segurança em Computação) da Universidade Federal de Santa Catarina tem desenvolvido vários trabalhos na área de segurança usando protocolos criptográficos[7]. Com base nos estudos das técnicas de segurança conhecidas na área de computação, este trabalho tem como objetivo apresentar um protocolo criptográfico que resolva os problemas relacionados à medição da efetividade dos anúncios bem como o cumprimento do contrato pelo sítio anunciante.

1.1 Objetivos

1.1.1 Objetivo Geral

Especificar, modelar, analisar e implementar um protocolo criptográfico para auditoria da publicidade na Web que permita medir a efetividade de uma campanha publicitária em termos de vendas bem como medir a se a publicação dos anúncios nos sítios contratados está sendo feita nos horários e com a freqüência previamente combinada.

[7] A criptografia que, de forma simplificada, pode ser entendida como um conjunto de técnicas que permite transmitir informações entre computadores de forma que sejam compreendidas apenas por pessoas autorizadas, será detalhada no capítulo 4.

1.1.2 Objetivos Específicos

Os objetivos específicos são os seguintes:

- Apresentar as formas de publicidade existentes na atualidade apontando as características (vantagens e desvantagens) de cada uma delas;
- Descrever os mecanismos comumente utilizados para publicação de anúncios na Web;
- Descrever os princípios básicos dos protocolos criptográficos, destacando as funcionalidades que serão usadas nesta proposta;
- Especificar o protocolo;
- Implementar uma versão simplificada do protocolo através de um projeto conjunto com alunos de graduação da Universidade Federal de Santa Catarina.

1.2 Motivação

A idéia de escrever sobre um protocolo criptográfico voltado à publicidade na Web surgiu a partir de um trabalho proposto numa disciplina de Segurança em Redes do Centro de Pós-Graduação da Universidade Federal de Santa Catarina em março de 2001. Este trabalho pedia a análise crítica de um artigo cujo teor era a proposta de uso de cupons eletrônicos para medir a efetividade de anúncios publicados na Web. O artigo analisado, escrito por Markus Jakobsson et al., [JAK 99], revelou-se um tema importante e ainda pouco explorado.

As pesquisas feitas a partir daí demonstraram que o problema da medição de audiência na Internet (e também da efetividade dos anúncios) não só ainda carece de propostas mais consistentes como também várias outras questões relacionadas à publicação de anúncios neste meio ainda não possuem solução. Uma destas questões está relacionada ao controle sobre a publicação dos anúncios, ou seja, a garantia de que o sítio contratado para publicá-los o esteja fazendo realmente com a freqüência e da forma combinada.

Por estes motivos, o tema despertou minha curiosidade e motivou-me a buscar a elaboração de uma solução para o assunto através desta dissertação de mestrado.

Além de ser um tema com grande potencial a ser pesquisado, ele enquadra-se diretamente na área de segurança e criptografia de dados, uma área fascinante e de grande relevância na atualidade onde cada vez mais as informações deixam de constar no papel para serem transmitidas através das redes de comunicação de dados.

O apoio do professor Ricardo Felipe Custódio para o desenvolvimento deste trabalho resultou ainda na criação de um projeto conjunto com alunos da graduação em Bacharelado em Ciência da Computação o que resultou na consistência ainda maior da proposta aqui apresentada.

1.3 Metodologias e Ferramentas

Para a realização deste trabalho será feito um levantamento bibliográfico relacionado primeiramente à área de publicidade e propaganda de modo a esclarecer a terminologia usada bem como os métodos e técnicas empregados para resolver questões de medição ligadas à publicação de anúncios.

Uma pesquisa abrangente sobre as tecnologias de segurança em computação disponíveis para o emprego em transações eletrônicas seguras também será necessária.

A implementação de um protótipo do protocolo será desenvolvida num projeto conjunto com alunos do curso de Bacharelado em Ciência da Computação, onde serão usadas tecnologias de desenvolvimento para Web as quais serão detalhadas mais adiante.

1.4 Terminologia

O protocolo proposto fará uso de diversos termos estão descritos a seguir de forma sucinta. Seu detalhamento será feito no decorrer deste documento onde se fizer necessário.

Empresa: diz respeito à empresa que tem interesse em anunciar seus produtos e serviços na Internet; é a "parte" interessada em anunciar;

Agência de publicidade: entidade que é contratada pela empresa para viabilizar o anúncio de seus produtos e serviços. Na maioria dos casos este papel é representado por uma empresa distinta especializada em publicidade. Porém, algumas vezes, pode ser assumido por um departamento da própria empresa que pretende anunciar seus produtos/serviços;

Sítio Anunciante: página da Internet onde os anúncios serão publicados. Dependendo da estratégia usada pela agência de publicidade, podem ser inúmeros os sítios escolhidos para divulgação;

Cliente: refere-se ao usuário da Internet que é alvo da empresa como potencial comprador;

Cupom eletrônico: documento eletrônico equivalente aos cupons de desconto usados no mundo real e que, após serem distribuídos, permitem aos clientes que obtenham vantagens na compra de bens ou serviços;

Autoridade Certificadora: parte confiável que tem a responsabilidade de emitir certificados que confirmam a assinatura digital de uma pessoa ou empresa;

Protocoladora Digital de Documentos Eletrônicos: parte confiável que tem a responsabilidade de datar documentos eletrônicos confirmando assim sua existência em determinado instante do tempo.

1.5 Requisitos

O protocolo criptográfico deve estar de acordo com os seguintes requisitos básicos:

1. **Efetividade para a empresa:** A **empresa** precisa saber se os anúncios publicados atingem os objetivos de divulgação revertendo-se em vendas e/ou contratações de

seus produtos/serviços;

2. **Efetividade para a agência de publicidade:** A **agência de publicidade** também precisa receber a informação sobre a efetividade dos anúncios publicados num **sítio anunciante** pois seu objetivo é indicar para a **empresa** os melhores locais para exibir seus anúncios; a fidelidade desta informação implica diretamente na confiabilidade da **agência de publicidade** perante a **empresa**;

3. **Efetividade para o sítio anunciante:** O **sítio anunciante** também precisa saber o grau de efetividade dos anúncios publicados de modo a poder medir o quanto pode cobrar pelo seu espaço de anúncio em contratos futuros de publicidade;

4. **Vantagem para o cliente:** Do ponto de vista do **cliente**, o objetivo é encontrar os produtos/serviços que lhe ofereçam as melhores vantagens;

5. **Auditoria do contrato de publicidade:** Outra característica importante do ponto de vista da **empresa** e também da **agência de publicidade** é a garantia de que o contrato com o **sítio anunciante** esteja sendo cumprido, isto é, que o anúncio esteja sendo publicado com a freqüência e durante o tempo que foi contratado;

6. **Medição da audiência:** O **sítio anunciante** tem interesse em comprovar sua audiência de modo a valorizar a oferta pelo seu espaço de publicidade;

7. **Privacidade do cliente:** Os dados pessoais do **cliente** não devem ser publicados em nenhum momento durante a execução das etapas do protocolo;

8. **Proteção dos participantes:** O protocolo deve proteger todos os participantes envolvidos (**empresa**, **agência de publicidade**, **sítio anunciante** e **cliente**) de qualquer fraude que possa ser originada por outro participante ou mesmo de um oponente externo.

1.6 Conteúdo do Documento

Este documento está estruturado da seguinte forma: o capítulo 2 detalha as formas de publicidade existentes na atualidade apontando as características (vantagens/desvantagens) de cada uma delas e também os métodos de aferição de audiência mais relevantes; o capítulo 3 apresenta os mecanismos comumente utilizados para medir a publicidade na Web (com destaque para a proposta de cupons eletrônicos) indicando seus pontos vulneráveis com relação à segurança; o capítulo 4 mostra as técnicas modernas de segurança utilizadas na elaboração de protocolos criptográficos; na seqüência, o capítulo 5 apresenta a proposta de um protocolo criptográfico para auditoria da publicidade na Web, que é o objetivo principal deste trabalho; finalmente, o capítulo 6 descreve como foi feito o projeto que implementou o protocolo.

Capítulo 2

Publicidade e Propaganda

2.1 Introdução

A compreensão das terminologias usadas na área de Publicidade e Propaganda é imprescindível para o desenvolvimento de um trabalho que esteja tão fortemente ligado a este tema.

Assim sendo, este capítulo pretende apresentar os princípios básicos da Publicidade e Propaganda descrevendo os meios de comunicação usados, a função de uma agência de publicidade e os métodos de aferição.

O objetivo é descrever como a publicidade funciona, enfocando principalmente outros meios de comunicação que não a Internet. Seria a descrição do que, neste trabalho, denominamos “publicidade convencional”, a qual estamos tratando como “toda forma de publicidade que não esteja ligadas à Internet”.

O entendimento claro deste tema auxiliará na compreensão da proposta desenvolvida neste trabalho.

A seção 2.2 deste capítulo apresentará os principais meios de comunicação e suas características. A seção 2.3 descreverá o papel das agências de publicidade. Em seguida, a seção 2.4 irá apresentar os principais métodos de medição relacionados à área de publicidade e propaganda.

2.2 Os Meios de Comunicação

Na área da publicidade e propaganda, os meios de comunicação que divulgam os produtos e/ou serviços de uma empresa são chamados simplesmente de **mídia**. O termo vem do inglês *media* conforme define Martins em [MAR 99]. Este autor afirma ainda que *"todo e qualquer lugar onde pudermos colocar uma mensagem publicitária deve ser considerado um meio de comunicação. De brinde promocional a uma rede nacional de televisão, tudo é mídia"*.

De uma forma mais genérica, pode-se classificar os tipos de mídia em **mídia eletrônica**, como é o caso do rádio e da televisão; **mídia impressa**, como jornais, revistas, *outdoors* e folhetos; **mídia alternativa**, quando se trata de brindes promocionais, balões, faixas de ruas, entre outros; **mídia digital**, onde enquadram-se jogos eletrônicos, CD-ROMs e a própria Internet de uma maneira geral [FER 99].

As informações acerca das principais mídias usadas na publicidade podem ser encontradas em diversas literaturas desta área. Abaixo, são descritas algumas mídias mais significativas conforme [PRE 00]:

Televisão é o meio de comunicação de maior penetração no mercado brasileiro (estima-se em 35 milhões o total de domicílios com televisão no Brasil - um dos maiores mercados do mundo); são cerca de 350 emissoras de TV cobrindo o território nacional; a televisão possui um alto desempenho em praticamente todos os segmentos porém o custo de publicidade é um dos mais altos;

Rádio também enquadrado como um dos grandes meios de comunicação de massa (estima-se que 90% dos domicílios brasileiros possuem pelo menos um aparelho de rádio), sua cobertura é geralmente regionalizada; o rádio pode apresentar-se em variadas versões, podendo acompanhar o ouvinte em seu automóvel, em pequenos aparelhos portáteis, em esperas telefônicas, em som ambiente, entre outras possibilidades; uma das vantagens de anunciar neste tipo de mídia refere-se à agilidade tanto na criação quanto numa possível mudança de um anúncio; outra vantagem diz respeito aos custos de publicidade que são bem menores se comparados aos da

televisão; em contrapartida, o nível de audiência não é tão significativo quanto o da televisão além de não possuir as mesmas características multimídias;

Jornal apesar de existirem cerca de 2.500 títulos de jornais no Brasil, a maior penetração desta mídia é registrada nas classes sócio-econômicas A e B; na maioria das vezes possui apenas cobertura local; em geral, possui algumas limitações com relação à qualidade de impressão;

Revista o mercado brasileiro de revistas está estimado em cerca de 1.500 títulos diversos; possuem gêneros variados que atingem uma grande variedade de público, desde revistas em quadrinhos, passando por informática, horóscopo, música, moda, turismo e muitos outros; tal como os jornais, sua maior penetração está nas classes sócio-econômicas A e B; geralmente permitem uma boa qualidade de impressão de anúncios, porém sua periodicidade é geralmente baixa (semanal/mensal);

Cinema mais de 900 salas em todo país são comercializadas por sete empresas exibidoras. As mudanças ocorridas na "indústria do entretenimento" nos últimos tempos têm transformado este meio num canal de comunicação eficaz, atingindo especialmente o público jovem, das classes A e B, residentes nas áreas urbanas;

Além das mídias citadas anteriormente, os autores mencionam outras menos conhecidas mas não menos relevantes:

out-of-home - OOH é um tipo de mídia cujo representante mais conhecido é o *outdoor*; abrange também placas sinalizadoras de ruas, letreiros luminosos, *busdoors*, cartazes em pontos de ônibus, adesivos e diversas outras alternativas similares.

TV por assinatura envolve as opções de TV paga ou TV à cabo, cujas coberturas podem ser até internacionais; tem a característica de atingir especialmente as classes mais altas, o que pode ser uma desvantagem do ponto de vista de abrangência.

Mídia digital engloba todos os recursos de comunicação viabilizados digitalmente tais como jogos eletrônicos, painéis eletrônicos, cd-roms, protetores de tela, entre out-

ros; seu maior representante hoje é a Internet cujo número de usuários ainda continua crescendo.

Em termos de credibilidade dos meios de comunicação, uma pesquisa do Instituto Datafolha realizada em julho de 2001, apresentou os seguintes resultados mostrados na tabela 2.1. A pesquisa foi feita com 1605 entrevistados em quatro capitais brasileiras mais o Distrito Federal ([dPD 01]).

Tabela 2.1: Credibilidade dos Meios de Comunicação.

Meio de Comunicação	Percentual
TV aberta	30%
Jornais	29%
Rádio	18%
Internet	10%
TV por assinatura	3%
Revistas	3%
Outros	7%

Fonte: Pesquisa Datafolha - Brasil - julho/2001 - em [dPD 01].

2.3 Agências de Publicidade

Uma agência de publicidade é uma prestadora de serviços em comunicação. Ela tem o papel de *"estudar o mercado do anunciante, o perfil sócio-econômico e comportamental do público-alvo e mais uma série de variáveis para, finalmente, fazer uma proposta de ação..."* [MAR 99]. A agência também é responsável pela criação e desenvolvimento das peças necessárias a uma campanha publicitária (comerciais de TV e rádio, anúncios de jornais e revistas e outros). Porém, a execução destas peças ficará a cargo de outras empresas denominadas, no meio publicitário, de **"fornecedores"**. Estas empresas

constituem-se nas gráficas, produtoras de vídeo e áudio, estúdios fotográficos e diversas outras prestadoras de serviços de apoio à atividade de propaganda. Na seqüência, a agência faz contato com os **veículos de comunicação** onde os anúncios produzidos serão distribuídos conforme a freqüência e intensidade estabelecidos como metas no planejamento da campanha.

Além da responsabilidade pela criação de uma campanha publicitária, pela sua produção (direta ou indiretamente) e pela sua veiculação, uma agência de publicidade também pode assumir o papel de promoção de vendas e de pesquisa de mercado. A promoção de vendas está ligada a estratégias como prêmios, concursos, degustação, entre outras. A pesquisa de mercado têm relação com a coleta de informações acerca do público-alvo e das estatísticas provenientes destas informações.

2.4 Métodos de Aferição de Audiência e Controle

Quando se fala de mídia convencional, existem diversos órgãos responsáveis pela aferição de resultados tais como índice de audiência, grau de penetração conforme o público-alvo, atividade em mídia das empresas concorrentes, entre outros. A tabela 2.2 apresenta um resumo dos principais institutos responsáveis por esta aferição no Brasil [PRE 00].

Outra informação importante fornecida por estes e outros órgãos é o controle da veiculação dos anúncios. Neste caso, o objetivo é certificar-se de que o veículo de comunicação escolhido cumpriu sua parte do contrato, exibindo os anúncios nos locais e/ou horários pré-estabelecidos, quando for o caso.

2.4.1 Medição de Audiência

Quanto à medição de audiência há diferentes métodos utilizados conforme o meio de comunicação. Estes métodos serão descritos nesta seção.

Tabela 2.2: Institutos de Aferição de Audiência. Principais mídias existentes com os respectivos institutos responsáveis pela aferição de resultados destas mídias e a periodicidade com que esta aferição é feita.

Mídia	**Instituto**	**Periodicidade**
Televisão	Ibope	Contínuo (diário)
	Marplan	Trimestral/Anual
Rádio	Ibope	Mensal
	Marplan	Trimestral/Anual
Jornal	Marplan	Trimestral/Anual
	Ibope	Trimestral
	IVC	Mensal
Revistas	Marplan	Trimestral/Anual
	IVC	Mensal
	Ibope	Não definida

Fonte: Predebon et al. ([PRE 00]).

2.4.1.1 Audiência da Televisão

Em termos de Brasil, o Ibope é referência unânime em termos de pesquisas de opinião de um modo geral. Por isso, citaremos aqui algumas das técnicas usadas por este instituto e mencionadas em [MAR 99].

Entrevista pessoal O tipo mais básico de pesquisa é a entrevista pessoal, onde os entrevistadores saem a campo coletando informações mediante contato direto com as pessoas; apesar de parecer um tanto rudimentar, ainda é uma estratégia comumente utilizada.

People-meter trata-se de um aparelho instalado em residências de centenas de famílias para medir especificamente a audiência da televisão fornecendo informações "on-line"; este tipo de medição é feito apenas em algumas das principais cidades brasileiras.

Pesquisa “caderno” ocorre como meio de substituição do *people-meter* nos locais ainda não ligados a este sistema; neste caso as famílias participantes preenchem planilhas especiais que são recolhidas semanalmente e cujos dados são computados por leitura óptica.

2.4.1.2 Audiência do Rádio

O rádio não dispõe ainda de meios sofisticados de aferição de audiência como acontece com a televisão. De forma geral, as pesquisas são baseadas em entrevistas e distribuídas em forma de relatórios periódicos.

2.4.1.3 Audiência de Jornais e Revistas

Além dos dados fornecidos pelo Ibope, os Estudos Marplan e o Instituto Verificador de Circulação são outros dois órgãos que fornecem dados confiáveis com relação à veiculação de jornais e revistas. As técnicas são baseadas em entrevistas além de auditoria de circulação e tiragem.

2.4.2 Controle de Veiculação dos Anúncios

Para a empresa que contrata os serviços de uma agência de publicidade e que geralmente faz um bom investimento neste serviço é muito importante certificar-se de que seu comercial está sendo veiculado nos horários e na forma previamente contratados. Para assegurar-se de que o anunciante está cumprindo com o contrato, existem serviços de fiscalização de veiculação em rádio e TV. No caso do Ibope, há um sistema computadorizado que “assiste” aos comerciais que vão ao ar e registram detalhadamente o horário em que foi exibido e se a exibição foi feita de maneira imperfeita.

2.5 Conclusão

Em termos de publicidade convencional (aqui tratada como a propaganda fora da Internet) percebe-se um sistema já consolidado tanto em relação aos estu-

dos das diversas mídias quanto aos métodos de aferição de audiência e auditoria. Quando trata-se da televisão, que é um dos meios de comunicação mais almejados pelas empresas anunciantes, estes métodos são ainda mais contundentes.

As agências de publicidade possuem atualmente diversos mecanismos que auxiliam na tomada de decisão quanto à escolha dos melhores veículos para atingir os objetivos almejados por seus clientes, bem como no controle sobre os anúncios publicados e os resultados alcançados.

Como veremos adiante neste trabalho, quando se trata de publicidade na Internet os métodos não estão consolidados e há muito ainda a ser pesquisado e desenvolvido.

Capítulo 3

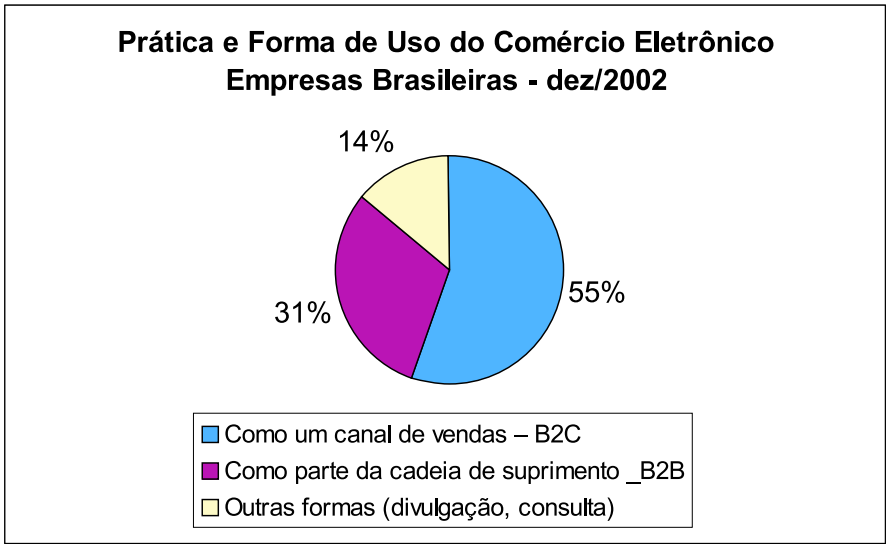
Publicidade na Web

3.1 Introdução

Uma das principais vantagens de usar a Web como meio de publicidade é a facilidade de interação com o cliente. Esta interatividade é um dos destaques desta mídia pois nenhum outro meio de comunicação de massa possui esta característica de forma tão dinâmica e direta. Ao visitar um sítio da Internet, um cliente pode navegar através do mesmo de forma totalmente livre. Ele próprio escolhe o que quer ver, quando quer ver, além de, muitas vezes, poder comprar diretamente e até mesmo acompanhar o andamento de seu pedido.

A importância da a Internet como meio utilizado para divulgar produtos e fazer negócios pode ser constatada no gráfico apresentado na figura 3.1. Dentre as empresas que usam a Internet para fazer algum tipo de negócio, mais da metade utiliza a forma de comércio direto entre cliente e empresa, comumente chamada de B2C ou *Business-To-Customer*.

Outro fator muito atrativo para o uso da Web como mídia é o custo, geralmente mais baixo que a maioria dos outros meios de publicidade. Outro ponto positivo está relacionado à agilidade. A publicação de um anúncio no sítio da própria empresa que deseja expor seu produto é geralmente uma tarefa simples e rápida. Além disso, atualmente é muito comum que anúncios publicitários sejam criados através de computa-



Fonte: Ibope e-Solutions / Valor Econômico
dezembro/2002

Figura 3.1: Uso do Comércio Eletrônico no Brasil. O gráfico apresenta as principais formas de uso da Internet pelas empresas brasileiras, sendo que mais da metade delas (55%) utiliza a forma de negociação direta entre empresa e cliente (B2C).

dores, o que facilita ainda mais a sua publicação em qualquer sítio imediatamente após sua produção.

Apesar das evidentes vantagens de usar a Internet para este fim, alguns problemas ainda impedem muitas empresas de anunciar nesta mídia. Entre os problemas menos significativos estão a falta de conhecimento por parte de empresas e agências de publicidade sobre como explorar todo o potencial deste meio. Outro fator refere-se ao tipo de consumidor que tem acesso a esta tecnologia. A maior parte de internautas brasileiros concentra-se nas classes sociais mais altas (classes A e B)[1] e este tipo de propaganda pouco atinge outras camadas da população onde muitas vezes encontra-se o público-alvo de determinadas empresas.

No entanto, a limitação mais importante é a dificuldade de se alcançar meios seguros para medir o sucesso deste tipo de publicidade. Uma pesquisa feita pelo

[1]Segundo pesquisa Ibope de maio de 2001, 46% da população das classes A e B acessam a Internet[IBO 01].

Internet Advertising Bureau (IAB) em fevereiro de 2001 demonstrou que esta questão das métricas é a segunda maior preocupação entre as entidades que usam a Web para divulgação [BUR 01].

Com relação ao problema das métricas, podemos destacar especialmente a dificuldade em medir o nível de sucesso de uma campanha publicitária, ou seja, o quanto a publicidade incrementou o volume de vendas. Outro aspecto difícil de mensurar está relacionado ao cumprimento do contrato de publicação do anúncio em um sítio anunciante, isto é, como garantir que os anúncios estão sendo publicados no sítio nos horários estabelecidos e com a freqüência pré-determinada em contrato.

Questões relacionadas a métricas serão discutidas com maiores detalhes na seção 3.2 deste capítulo. Ali estarão detalhadas as técnicas de contagem de cliques e também de cupons eletrônicos.

3.2 Mecanismos de Medição

Conforme já foi citado, as métricas sobre a publicidade veiculada na Internet constituem-se num dos grandes desafios deste tipo de publicidade. Assim, alguns mecanismos de medição existentes serão descritos nesta seção.

Existem métodos alternativos de controle do sucesso de um anúncio como, por exemplo, comparar o aumento no volume de vendas após a publicidade. Outra alternativa é averiguar (através de visitas em intervalos freqüentes) se o anunciante está mesmo publicando seu anúncio como foi combinado. Como estes métodos são precários, a solução ideal deve basear-se em mecanismos automatizados que possam gerar tais resultados de forma eficiente e segura.

Aqui apresentaremos dois mecanismos de medição comumente que podem ser utilizados em transações que envolvem publicidade na Web: a técnica da contagem de cliques e o uso de cupons eletrônicos.

3.2.1 A Técnica da Contagem de Cliques

A taxa de contagem de cliques, também chamada de taxa de cliques, corresponde ao número de vezes que um usuário clica num anúncio ou *banner*. Este ato de clicar no anúncio leva o **cliente**, invariavelmente, ao sítio da **empresa** que anunciou seu produto/serviço. A taxa de cliques é calculada "pela divisão do número total de cliques pelo número de impressões[2] do anúncio numa dada campanha" [JÚN 00].

Quando se fala de medição do sucesso da publicidade na Web dois problemas comuns são detectados no uso da técnica de contagem de cliques:

- As **empresas** que solicitam a publicação dos anúncios podem negar o recebimento de visitas ao seus sítios; e
- Os **sítios anunciantes** podem simular falsas visitas (através de software especializado, por exemplo) para tirar vantagens com o suposto aumento da taxa de cliques.

Apesar de existirem estudos para evitar estes problemas, os meios empregados não garantem segurança total especialmente com relação à segunda questão.

3.2.2 Os Cupons Eletrônicos

O problema da medição de audiência na Web foi o alvo do artigo [JAK 99] onde é proposta uma estratégia de uso de cupons eletrônicos. Os autores iniciam demonstrando a importância da publicidade na Web bem como no mundo real e, em seguida, expõem o problema relacionado à dificuldade de medir o nível de sucesso de uma campanha publicitária feita na Internet. As questões colocadas pelos autores são as seguintes:

- Como saber se os **clientes** que visitaram o sítio da empresa chegaram ali através de um anúncio colocado em um **sítio anunciante**?
- Como saber quantas destas visitas estimuladas pelos anúncios obtiveram sucesso através de uma venda efetiva?

[2] A **impressão** é relativa às visualizações de um anúncio publicitário no sítio [JÚN 00].

- Como conseqüência destas respostas, quanto seria justo pagar ao **sítio anunciante** pelo sucesso da campanha?

- Como ter certeza de que as visitas ao sítio da **empresa** foram feitas por pessoas “de verdade” ou por um programa de computador que simula esta situação e gera um falso incremento de visitantes?

Para a primeira indagação, o método da contagem de cliques (descrito na seção anterior) permite identificar o número de vezes que um sítio foi acessado a partir de outro (que seria o **sítio anunciante**). Porém, esta técnica não permite responder a nenhuma das outras questões. Desta forma os autores propõem apresentar uma abordagem mais abrangente neste artigo.

Em comparação com a publicidade no “mundo real”, os cupons são lembrados como um meio de propaganda que traz vantagens tanto para os consumidores, beneficiando-os com descontos, promoções e outros incentivos, bem como à empresa que os oferece, que pode ter controle sobre o sucesso de sua campanha, quem são seus clientes, onde obtiveram os cupons e outras informações sobre estes clientes. Os cupons são anúncios promocionais geralmente impressos em jornais, revistas e outras mídias em papel que podem ser recortados pelos consumidores que, ao efetuarem suas compras nas lojas que promoveram o anúncio, podem trocá-los por brindes, descontos e outros bônus atrativos, dependendo da promoção descrita no cupom.

Outros autores também escreveram propostas que baseiam-se no uso de cupons eletrônicos. Entre eles destacamos Carlo Blundo et al. ([BLU 02]) que propôs melhorias à proposta de Jakobsson e também Rahul Garg at al. ([GAR 01]) que implementou um protótipo relatando algumas medidas de desempenho no uso de cupons eletrônicos.

A proposta é transpor para a Web este método de publicidade amplamente conhecido nos meios convencionais, denominando-o cupons eletrônicos. Além de conseguir *feedback* imediato sobre o sucesso de seus anúncios, as empresas poderiam obter informações precisas tais como a data e hora de acesso, o anunciante de onde o cupom foi obtido, além de poder controlar a segurança e a privacidade com técnicas es-

peciais disponíveis.

Em termos de confiabilidade, os autores destacam que sua proposta objetiva garantir que ambas as partes (**empresa** e **sítio anunciante**) possam saber o número de acessos dos **clientes** através do uso dos cupons, tendo controle sobre os custos dos anúncios. Esta proposta segue o que os autores chamam de modelo de mercado, onde nenhuma das partes se beneficiaria com possíveis trapaças pois elas seriam detectáveis.

3.2.3 O Esquema dos Cupons Eletrônicos

A figura 3.2 mostra um esquema simplificado para o uso dos cupons eletrônicos.

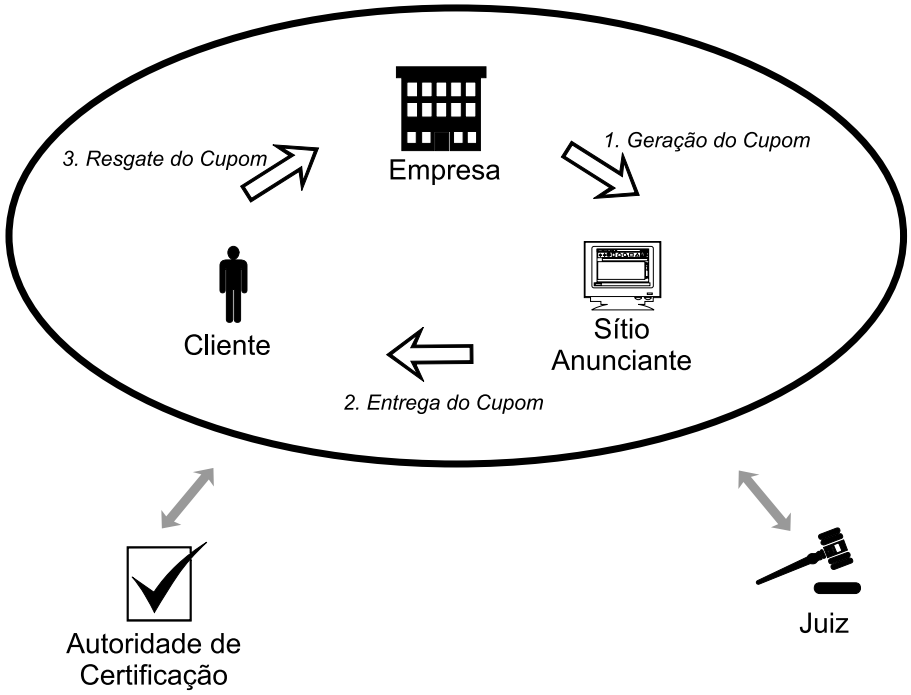


Figura 3.2: Esquema de cupons eletrônicos. O cupom é gerado pela empresa e repassado a sítio anunciante. Ao visitar a página do sítio o cliente recebe o cupom que pode, mais tarde, ser resgatado por ele e reverter-se em vantagens na compra de bens e serviços da empresa. O esquema também supõe o uso de uma **Autoridade Certificadora** e também de um **Juiz** (que teria a função de resolver eventuais litígios).

O esquema proposto por [JAK 99] propõe o uso de assinatura digital. Além disso, assumem que as **empresas** possuam certificados digitais de uma autoridade certificadora que, por sua vez, também usa um dos esquemas de assinatura mencionados.

O modelo proposto é composto das seguintes fases:

1. **Contratação:** Ambos, **empresa** e **sítio anunciante**, oferecem seus serviços em busca de acordos que podem ser formalizados em contratos. Estes contratos definem o preço a ser pago por uma campanha quer tenha sucesso ou não.

2. **Inicialização do contrato:** Ao iniciar um contrato de publicidade a **empresa** cria um anúncio como abaixo:

$$ANUNCIO = txt||advertiser\_id \tag{3.1}$$

onde

txt é a descrição da oferta da **empresa** com os termos de uso e

advertiser_id é um identificador único para o **sítio anunciante**.

Em seguida a **empresa** gera a assinatura A para criar o cupom, armazenando-o em seu banco de dados e enviando-o para o **sítio anunciante**:

$$C = A_{EMPRESA}(ANUNCIO) \tag{3.2}$$

O **sítio anunciante**, por sua vez, checa a assinatura e somente a aceita caso seja válida. Quando inválida, ele envia uma reclamação à **empresa** e a rejeita.

3. **Execução do contrato:** possui duas fases como descrito abaixo:

   - **Entrega do cupom:** quanto o **cliente** visita o **sítio anunciante**, este último seleciona um conjunto de cupons e os envia ao **cliente**, que os armazena o cupom C com o endereço do sítio visitado.

- **Resgate do cupom:** acontece quanto o **cliente** envia o cupom recebido anteriormente para a **empresa**, que checa a veracidade do cupom comparando-o com seu banco de dados. Se estiver tudo certo, o **cliente** poderá fazer uso da vantagem oferecida no cupom. Caso contrário, ele será notificado da falha e passa-se para a fase de detecção de corrupção.

4. **Detecção de corrupção:** quando detecta que um cupom recebido não está em sua base de dados porém possui uma assinatura válida, a **empresa** conclui que sua chave privada foi corrompida e que medidas de segurança devem ser tomadas. Caso contrário, ela simplesmente notifica o usuário de que o cupom não é válido. Caso não haja acordo entre as partes envolvidas, a figura de um **juiz** (definida como uma "terceira-parte confiável") pode ser acionada para resolver o litígio.

5. **Resumo dos benefícios do contrato:** sob o ponto de vista de cada participante:

   - **Para a empresa:** conta quantos usuários compraram seus produtos com os cupons e através de qual **sítio anunciante**, podendo comparar os benefícios com os preços pagos pelos anúncios.
   - **Para o sítio anunciante:** avalia, para cada **empresa**, o custo da campanha comparando-o com o valor recebido no início do contrato. Isto permite que ambos, **empresa** e **sítio anunciante**, reentrem na fase de contratação com informações mais precisas.
   - **Para o cliente:** avalia continuamente os benefícios oferecidos pelos anúncios, tal como os consumidores normalmente fazem no "mundo real".

6. **Resolução de conflito:** o **cliente** tem condições de averiguar se a assinatura e o certificado digitais de uma **empresa** são válidos caso ela rejeite um de seus cupons. Neste caso, o **cliente** tem provas de que seu cupom é válido e deve ser aceito. Se o certificado da **empresa** é inválido ou não existe, fica provado que ela é desonesta. Se o certificado é válido mas a assinatura não, fica provado que houve trapaça do **sítio anunciante** que forneceu o cupom.

3.3 Conclusão

Alguns métodos usados para resolver o problema da medição de audiência na Web foram apresentados neste capítulo.

O método de contagem de cliques possui diversas vulnerabilidades e não garante, portanto, confiabilidade dos resultados obtidos

A estratégia de uso de cupons eletrônicos não garante apropriadamente a medição de audiência pois baseia-se na devolução de cupons distribuídos aos clientes. Como nem sempre os clientes terão interesse em resgatar as vantagens oferecidas pelos cupons, as empresas não terão a comprovação da efetividade de sua publicidade.

Observa-se, deste modo, uma carência no sentido de garantir às **empresas** que anunciam produtos/serviços dados confiáveis com relação à medição de audiência e também da efetividade de seus anúncios em termos de vendas.

Outro ponto muito importante situa-se no controle da veiculação dos anúncios dentro das condições estabelecidas em contrato (horários e freqüência de publicação) que não são garantidos por nenhuma das técnicas citadas e, portanto, carecem de algum mecanismo auxiliar para este gerenciamento.

Capítulo 4

Protocolos Criptográficos

4.1 Introdução

A segurança das informações armazenadas nos computadores bem como daquelas que transitam entre eles é um dos temas da maior relevância nos últimos tempos.

Com o advento das redes de computadores e depois, com a Internet, a possibilidade de que as informações que fluem entre eles possam ser lidas por pessoas não autorizadas deu origem a diversos estudos de onde nasceu a área da segurança em computação.

Neste capítulo serão descritos os princípios da área de segurança em computação e de como são construídos os protocolos criptográficos. A seção 4.2 apresentará uma visão geral sobre segurança; a seção 4.3 descreverá a criptografia de dados (simétrica e assimétrica); as funções de resumo serão descritas na seção 4.4; as técnicas de assinatura digital serão apresentadas na seção 4.5 e a seção seguinte, 4.6 descreverá os princípios uma Infra-estrutura de Chaves Públicas; o detalhamento de uma Protocoladora Digital de Documentos Eletrônicos será mostrado na seção 4.7.

4.2 Princípios de Segurança

A área de segurança em computação, especialmente a de segurança em redes busca garantir que informações que trafegam entre computadores não sejam acessadas, copiadas ou modificadas por pessoas que não tem autorização para tal. Para garantir a segurança das informações, deve-se partir de alguns requisitos básicos. Os requisitos básicos de segurança que poderiam ser exigidos para o uso de redes de computadores são [MEN 96]:

Confidencialidade: Garantir que tanto a informação armazenada em um sistema de computador quanto a informação transmitida sejam acessíveis apenas por pessoas autorizadas;

Integridade: Garantir que somente as partes autorizadas conseguirão realizar qualquer tipo de alteração nas informações de um sistema de computador;

Autenticação: Garantir que a origem de uma mensagem ou documento eletrônico está corretamente identificada, com a certeza de que a identidade não é falsa;

Não recusa: Assegurar que nem o remetente nem o destinatário de uma mensagem possam negar sua transmissão após tê-la feito;

Os items acima são também denominados **serviços de segurança**. A maioria destes serviços pode ser garantida através de uma técnica chamada criptografia, como será descrito na seção 4.3.

4.2.1 Ataques de Segurança

Todos os pressupostos de segurança baseiam-se na iminente possibilidade de ataques de pessoas não autorizadas. Há uma relação direta dos possíveis ataques de segurança com os serviços descritos na seção anterior. A descrição dos ataques pretende demonstrar o modo como os serviços de segurança podem ser ameaçados. A partir deste estudo é que os mecanismos de segurança são desenvolvidos.

Num sistema de computador, as informações fluem sempre de uma fonte de origem para um local de destino. Este fluxo de informações é conhecido como "fluxo normal". Durante este percurso a informação pode sofrer alguns ataques conforme descrito por Stallings [STA 99] e detalhado a seguir:

Interrupção: Ocorre quando um componente do sistema é destruído ou torna-se indisponível ou inutilizável. Pode ocorrer, por exemplo, com a destruição de um componente de *hardware* ou o corte de uma linha de comunicação;

Interceptação: Ocorre quando uma pessoa, programa ou um computador não autorizados obtêm acesso a informações podendo visualizá-las ou mesmo copiá-las ilicitamente. Este tipo de ataque diz respeito ao serviço de **confidencialidade**;

Modificação: Ocorre quando uma pessoa, programa ou computador não autorizados, além de obter acesso a uma informação, conseguem ainda modificá-la antes que chegue ao seu destino. Este tipo de ataque ameaça o serviço denominado **integridade**;

Fabricação: Ocorre quando uma informação falsificada é inserida num sistema. Esta inserção pode se dar em forma de uma mensagem enviada em uma rede simulando ser de uma pessoa autorizada ou através da adição de registros em um arquivo de acesso restrito. Este tipo de ataque atinge o serviço de **autenticidade**.

A figura 4.1 detalha cada um dos tipos de ameaças à segurança de um sistema.

4.3 Criptografia de Dados

Segundo o dicionário Aurélio [FER 99], *"criptografia é a arte de escrever em cifra ou em código"*. O objetivo é tornar uma informação incompreensível às pessoas não-autorizadas e permitir somente àquelas que detêm a chave que possam decifrá-la. Isto porque o segredo da criptografia baseia-se no uso de uma chave que é uma espécie de código secreto que, combinado à informação cifrada, permite decodificá-la.

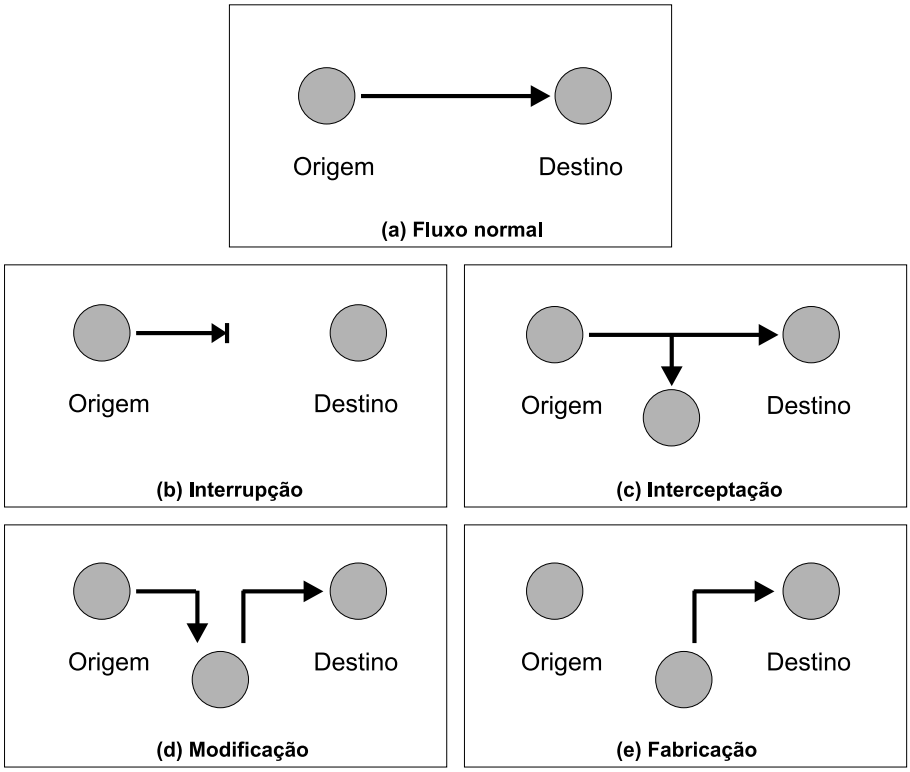


Figura 4.1: Tipos de Ataques. Esta figura apresenta os tipos de ataque possíveis a um sistema de computador. Ao topo, a figura (**a**) demonstra o fluxo normal de informações, quando não há nenhuma forma de interferência. As demais figuras (**b**, **c**, **d** e **e**) ilustram os diferentes tipos de ataques possíveis.

A criptografia é utilizada há muitos séculos e há registros de seu uso principalmente em tempos de guerra para troca de mensagens entre tropas de forma a garantir que, caso interceptada, a mensagem não pudesse ser compreendida pelos inimigos.

Com o advento da informática e principalmente das redes de computadores, diversos métodos de criptografia de dados passaram a ser desenvolvidos.

A criptografia é uma técnica que permite a implementação dos serviços de segurança descritos na seção 4.2): **confidencialidade**, **autenticação**, **integridade** e **não recusa**.

De uma forma geral, a criptografia de dados pode ser dividida em dois tipos básicos: a **criptografia simétrica** e a **criptografia assimétrica** que serão descritas nas próximas seções.

4.3.1 Criptografia Simétrica

A criptografia simétrica, também chamada **criptografia convencional**, supõe o uso de **uma única chave** tanto para cifrar quanto para decifrar uma informação. Isto exige que ambos, remetente e destinatário de uma mensagem, combinem esta chave entre si e transmitam-na através de algum meio seguro[1].

Outra característica da criptografia simétrica é o fato de serem necessários dois algoritmos para efetuar a transmissão sigilosa de informações: um **algoritmo de cifragem** e outro **algoritmo de decifragem**. Ambos os algoritmos devem ser construídos de modo que, usando a mesma chave, possam atingir seus objetivos.

Sendo assim, supondo uma mensagem original **X**, enviada de um remetente para um destinatário qualquer, e uma chave secreta **K** compartilhada entre eles, podemos usar um algoritmo de cifragem **C** para criar o texto cifrado **Y**:

$$Y = C_K(X)$$

Quando o texto cifrado **Y** chega ao destinatário, ele é decifrado com o algoritmo **D** usando a mesma chave **K** de modo a obter-se novamente a mensagem original **X**:

$$X = D_K(Y)$$

A figura 4.2 ilustra de forma simplificada o esquema de funcionamento da criptografia simétrica.

Diversos algoritmos de criptografia simétrica foram desenvolvidos e são todos amplamente conhecidos. Seu código é aberto para o conhecimento de todos. Entre os algoritmos de criptografia simétrica mais conhecidos estão:

DES: Data Encryption Standard e suas variações como **Double DES** e **Triple DES** cujo detalhamento pode ser encontrado em [STI 95] e em inúmeras outras referências;

AES: Advanced Encryption Standard que está descrito em [NEC 00];

[1] A chave secreta pode ser transmitida entre os participantes de diversos modos: pode ser através de um contato pessoal, via telefone, pelo correio convencional ou usando algumas técnicas especiais que podem ser encontradas na seção 5.3 do livro de William Stallings [STA 99].

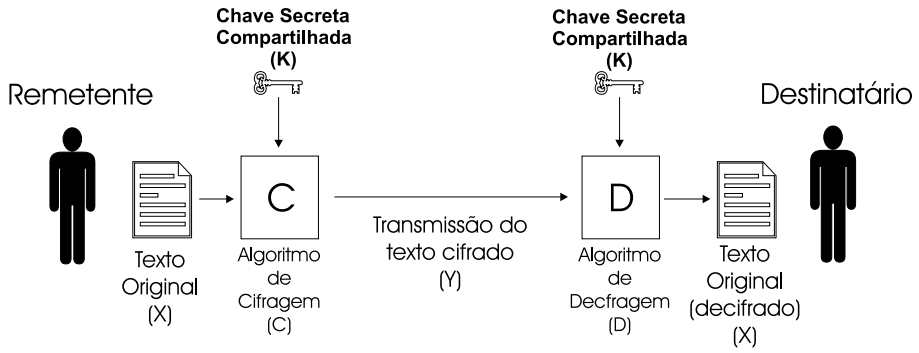


Figura 4.2: Criptografia Simétrica. Na criptografia simétrica, o texto **X** enviado pelo remetente passa por um algoritmo de cifragem **C** usando uma chave secreta compartilhada **K** garantindo que, ainda que interceptado, seu conteúdo não será compreensível. Ao chegar ao destinatário o texto cifrado **Y** passa pelo processo de decifragem **D** que, usando a mesma chave **K**, permitirá que ele torne-se novamente legível. A chave secreta **K** deve ser conhecida tanto pelo remetente quanto pelo destinatário.

IDEA: International Data Encryption Algorithm proposto originalmente em [LAI 90] e revisado posteriormente em [LAI 91];

Blowfish: Desenvolvido por Bruce Schneier cujos detalhes podem ser encontrados em [SCH 93] e [SCH 96];

RC5: Criado por Ron Rivest e descrito em [RIV 94];

Nos algoritmos usados na criptografia simétrica, o segredo estará unicamente na chave. A segurança pode ser melhorada com o aumento no tamanho da chave, ou seja, no número de *bytes* de que é composta. Quanto maior for o tamanho da chave, mais difícil será para um possível intruso descobri-la (ou deduzi-la) para decifrar o texto cifrado.

4.3.2 Criptografia Assimétrica

A criptografia assimétrica, também conhecida como **criptografia de chave pública** usa técnicas modernas baseadas em funções matemáticas para alcançar seu objetivo. Uma importante característica da criptografia assimétrica é o fato de utilizar

duas chaves diferentes, ao contrário da criptografia simétrica que usa uma única chave compartilhada.

Na criptografia assimétrica, as duas chaves usadas por cada participante são denominadas respectivamente como **chave pública** e **chave privada**. A chave pública é distribuída abertamente a qualquer pessoa. Pode ser publicada em catálogos, em sítios da Internet, enfim, deve se tornar conhecida de todos. A chave privada, ao contrário, deve ser sigilosa e só pode ser conhecida pelo seu proprietário.

O mecanismo da criptografia assimétrica prevê o uso das duas chaves de duas possíveis formas:

1. Quando uma mensagem (**X**) é cifrada (**C**) com a chave privada de uma pessoa (**KR**), ela só pode ser decifrada (**D**) com a chave pública desta pessoa (**KU**):

   $Y = C_{KU}(X)$
   $X = D_{KR}(Y)$

2. Quando uma mensagem (**X**) é cifrada (**C**) com a chave pública de uma pessoa (**KU**), ela só pode ser decifrada (**D**) com a chave privada desta pessoa (**KR**):

   $Y = C_{KR}(X)$
   $X = D_{KU}(Y)$

Assim, supondo-se dois participantes de um sistema de comunicação denominados Alice (**A**) e Beto (**B**), sendo **A** o remetente de uma mensagem e **B** o destinatário da mesma, pode-se deduzir que na criptografia assimétrica:

- Uma mensagem cifrada (**Y**) com a chave privada de **A** (KR_A) poderá ser decifrada por **B**, ou por qualquer outra pessoa, usando a chave pública de **A** (KU_A):

  $Y = C_{KR_A}(X)$
  $X = D_{KU_A}(Y)$

  A figura 4.3 mostra este modelo de criptografia assimétrica que garante a autenticação. Este modelo é utilizado principalmente em **assinaturas digitais** conforme descrito na seção 4.5.

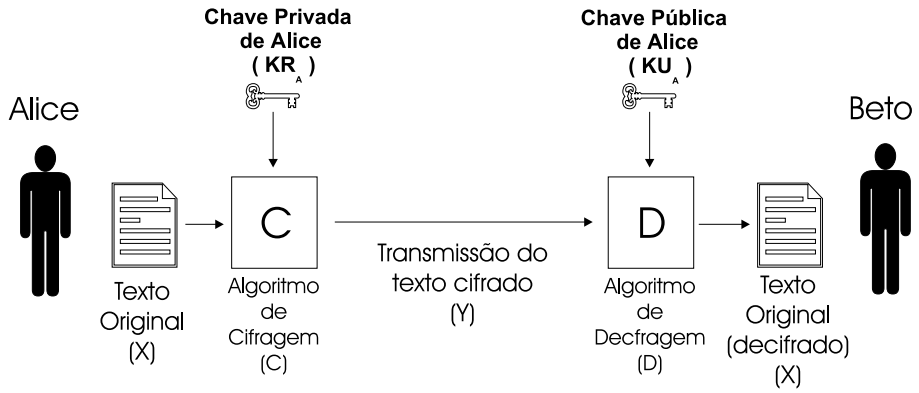


Figura 4.3: Criptografia Assimétrica: Autenticação. O esquema acima mostra um texto enviado por Alice que passa por um algoritmo de cifragem (**C**) com a chave privada da própria Alice (KR_A). Após ser transmitido para Beto, o texto cifrado **Y** passa pelo processo de decifragem (**D**) usando a chave pública de Alice (KU_A) permitindo que ele torne-se novamente legível. Este modelo garante apenas a **autenticação** (e não a confidencialidade) pois qualquer pessoa que intercepte o texto durante a sua transmissão poderá decifrar a mensagem de Alice usando a **chave pública** dela já que esta chave é de conhecimento público, como o próprio nome sugere.

- De outra forma, uma mensagem cifrada (**Z**) com a chave pública de **B** (KU_B) só poderá ser decifrada por **B** com a sua própria chave privada (KR_B); isto significa que qualquer outra pessoa que eventualmente tenha acesso a essa mensagem não conseguirá decifrá-la pois precisaria, para isso, da chave privada de **B** (que é de conhecimento exclusivamente dele):

  $Z = C_{KU_B}(X)$
  $X = D_{KR_B}(Z)$

  A figura 4.4 mostra este modelo de criptografia assimétrica que garante a confidencialidade.

As duas formas de uso da criptografia assimétrica descritas anteriormente podem levar a falsa impressão de que ela é insuficiente pois, quando garante autenticação não garante confidencialidade e vice-versa. No entanto, estas são apenas as duas formas básicas distintas no uso da criptografia assimétrica. Pode-se assegurar tanto a confidencialidade quanto a autenticação a partir da combinação entre estas duas formas. Os detalhes acerca destas possibilidades podem ser encontrados em Stallings

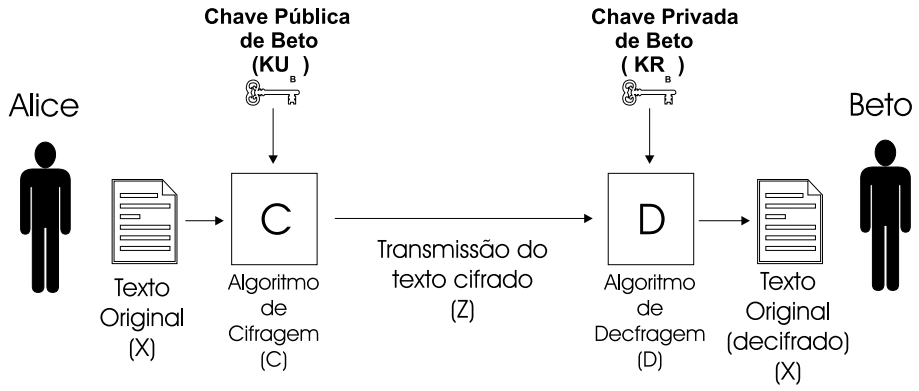


Figura 4.4: Criptografia Assimétrica: Confidencialidade. Esta figura mostra um texto **X** enviado por Alice que passa por um algoritmo de cifragem (**C**) com a chave pública de Beto (KU_B). Após ser transmitido para Beto, o texto cifrado **Z** passa pelo processo de decifragem (**D**) usando a chave privada do próprio Beto (KR_B), tornando-o legível novamente. Este modelo garante apenas a **confidencialidade** (e não a autenticação) pois se o texto for interceptado durante a sua transmissão ele só poderá ser decifrado com a **chave privada** de Beto que deve estar em posse dele exclusivamente.

[STA 99].

Como na criptografia simétrica, o eficácia da criptografia assimétrica está no tamanho da chave pois os algoritmos também são de conhecimento público. Outro fator importante é manter em sigilo a chave privada, divulgando apenas a chave pública. Entre os algoritmos mais difundidos de criptografia assimétrica podem ser citados:

RSA: **R**ivest, **S**hamir e **A**dleman; algoritmo desenvolvido pelos três cientistas que deram a ele as iniciais de seus nomes e publicado em [RIV 78];

Diffie-Hellman: criado para permitir troca de chaves entre participantes de um sistema de comunicação e proposto em [DIF 76];

ECC: Elliptic Curve Cryptography; algoritmo mais recente baseado num princípio matemático denominado curvas elípticas cuja descrição em detalhes pode ser encontrada em [MEN 93];

Estudos feitos a partir dos algoritmos de criptografia assimétrica demonstram que o aumento no tamanho das chaves usadas podem tornar a segurança praticamente inviolável [STA 99]. Porém, neste caso, a complexidade de execução dos al-

goritmos se torna progressivamente maior. Esta característica resulta, portanto, numa diminuição da performance à medida que se aumenta o tamanho da chave. Por isso, o uso da criptografia assimétrica é aplicada de forma mais restrita, principalmente para **assinatura digital** (seção 4.5) e **troca de chaves**.

Maiores detalhes sobre criptografia assimétrica podem ser encontrados em [STI 95], [SCH 96] e [MEN 96].

4.4 Funções de Resumo

As funções de resumo são ítens de grande relevância na área da criptografia. Seu objetivo é o de criar um resumo de tamanho pré-fixado a partir de uma mensagem qualquer.

Uma função resumo **R** pode ser aplicada sobre uma mensagem **M** qualquer (independentemente do tamanho de **M**) de forma a gerar um valor de resumo **r** cujo tamanho é fixo:

$$r = R(M)$$

Nechvatal em [NEC 91] descreve as seguintes propriedades desejáveis para funções de resumo:

1. a função **R** pode ser aplicada ao um bloco de dados de qualquer tamanho;
2. a função **R** sempre deve produzir uma saída de tamanho pré-fixado;
3. a função **R(M)** deve ser relativamente fácil de ser implementada para qualquer mensagem **M**;
4. deve ser inviável obter a mensagem **M** a partir de seu resumo **r**;
5. para duas mensagem **M** e **N** diferentes não deve ser possível encontrar o mesmo valor de resumo **r**, ou seja, $R(M) \neq R(N)$.

Um dos objetivos do uso de funções de resumo é integridade de dados. Quando uma função de resumo é aplicada sobre um bloco de dados pode-se, mais tarde,

garantir que ele não sofreu nenhuma alteração calculando-se novamente o valor do resumo. Se o valor do segundo resumo for igual ao primeiro significa que a mensagem não sofreu nenhuma alteração. Dessa forma, pode-se usar funções de resumo para autenticar mensagens, ou seja, garantir ao destinatário que a mensagem recebida não sofreu nenhuma alteração durante sua transmissão.

As funções de resumo são amplamente utilizadas em conjunto com técnicas de criptografia como, por exemplo, com assinaturas digitais que serão descritas a seguir.

Alguns exemplos de funções de resumo amplamente conhecidas são:

MD4: Criado por Ronald L. Rivest em 1990 e descrito no documento RFC 1320 [RIV 92a];

MD5: Ronald L. Rivest publicou a descrição detalhada do sucessor do MD4 em [RIV 92b];

SHA-1: foi desenvolvido no órgão americano NIST (*National Institute of Standards and Technology*) e publicado como padrão no documento [Nat 95];

RIPEMD-160: desenvolvido na Europa através do projeto RIPE (*RACE Integrity Primitives Evaluation*) e publicado no documento [DOB 96], sucedeu uma versão anterior denominada simplesmente RIPEMD.

Maiores detalhes sobre funções de resumo podem ser encontrados em diversas referências importantes como [STI 95], [SCH 96], [MEN 96] e [NEC 91].

4.5 Assinatura Digital

Uma assinatura digital tem o mesmo objetivo de uma assinatura manuscrita em papel: garantir a identificação do autor do documento. Em outras palavras, garantir a autenticidade do documento. Entretanto, considerando o meio eletrônico de transmissão de documentos assinados, deve-se empregar técnicas para garantir a integridade e autenticidade de tais documentos.

Segundo Menezes em [MEN 96], a “assinatura digital de uma mensagem é um número que depende de um valor secreto conhecido apenas pelo próprio assinante e do conteúdo da própria mensagem assinada”.

O conceito de assinatura digital foi introduzido em 1976 por Diffie e Hellman em [DIF 76] embora a primeira realização prática tenha aparecido em [RIV 78].

Existem alguns esquemas de assinatura digital que usam criptografia simétrica (uma única chave secreta compartilhada) mas a maior parte deles usa criptografia assimétrica (também chamada criptografia de chave pública). Aqui descreveremos apenas o segundo e mais difundido tipo.

Usando a mesma notação sugerida por Bruce Schneier em [SCH 96], a assinatura digital **S** de uma mensagem **M** qualquer usando uma chave **K** pode ser escrita como:

$$S_K(M)$$

E sua verificação (que pode ser feita pelo destinatário da mensagem, por exemplo):

$$V_K(M)$$

Existem diversos algoritmos de assinatura digital. Alguns deles (como o RSA, por exemplo) usam o mesmo princípio descrito na seção 4.3.2 que descreve a autenticação (figura 4.3).

Muitos esquemas de assinatura digital baseiam-se na cifragem do resumo da mensagem e não na cifragem da mensagem inteira. Em geral, esta opção diminui o esforço computacional necessário para a assinatura digital. A figura 4.5 mostra um exemplo deste tipo de assinatura.

Os principais algoritmos de assinatura digital são:

RSA: refere-se ao algoritmo de criptografia assimétrica criado por **R**ivest, **S**hamir e **A**dleman e descrito em [RIV 78];

Diffie-Hellman: proposto pelos mesmos autores que introduziram o conceito de assi-

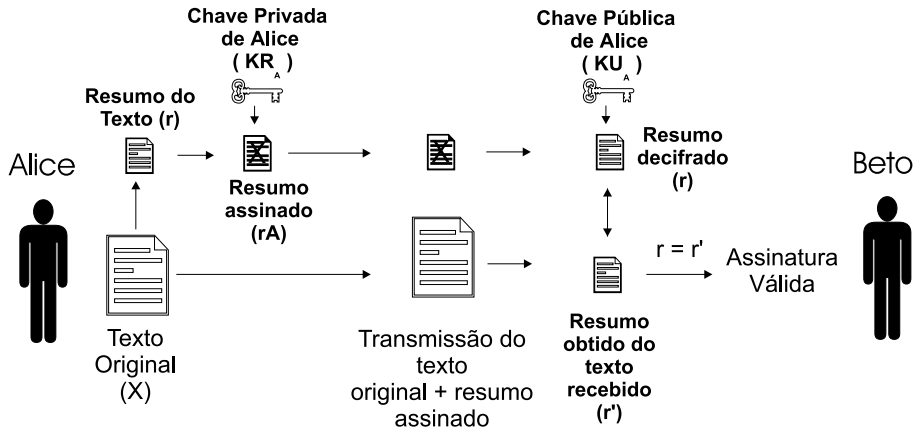


Figura 4.5: Exemplo de Assinatura Digital. Uma forma de assinar digitalmente é: criar um resumo do texto original, cifrar o resumo com a chave privada do remetente e enviar o resumo cifrado junto com o texto original. Ao receber estas informações, o destinatário pode verificar a assinatura desta forma: decifrar o resumo que recebeu com a chave pública do remetente, criar outro resumo a partir do texto original recebido e comparar ambos. Se forem idênticos a assinatura pode ser aceita como válida.

natura digital em [DIF 76];

DSA: o *Digital Signature Algorithm* é o algoritmo usado no esquema de assinatura digital padrão (DSS) proposto pelo órgão americano NIST (*National Institute of Standards and Technology*) e publicado no documento [Nat 94];

ElGamal: baseado em um problema matemático denominado logaritmos discretos e publicado em [ELG 85];

Schnorr: baseado em equações polinomiais, está descrito em [ONG 85];

Existem inúmeros outros algoritmos e esquemas de assinatura digital que os utilizam. Um estudo mais aprofundado pode ser feito através das referências já citadas nesta seção e dos livros clássicos como [STI 95], [SCH 96] e [MEN 96].

4.6 Infra-estrutura de Chaves Públicas - ICP

A criptografia assimétrica, pela sua característica de uso de múltiplas chaves, pode criar algumas dificuldades com relação ao gerenciamento das chaves. Isto

ocorre pelo fato de que cada pessoa tem um ar de chaves. Sendo assim, os principais questionamentos são:

- Como divulgar de forma eficiente as chaves públicas para que as outras pessoas tomem conhecimento delas?

- Como garantir que uma determinada chave é realmente a chave pública da pessoa com quem se deseja trocar mensagens cifradas?

Stallings [STA 99] cita quatro alternativas para solucionar o problema da distribuição de chaves públicas:

- **Divulgação Pública:** consiste em divulgar a chave pública por meios diversos de forma a torná-la conhecida por outras pessoas; o problema desta alternativa está na possibilidade de alguém se fazer passar por outra pessoa e anunciar sua própria chave pública, permitindo que ela receba mensagens em nome de outra até que sua fraude seja descoberta;

- **Diretório Público:** consiste em divulgar a chave pública através de uma entidade confiável que registraria as chaves públicas de pessoas conhecidas por ela e anunciaria a lista em meios de comunicação públicos; o problema consiste na possibilidade de um impostor, fazendo-se passar pela entidade do diretório público, divulgar falsas chaves públicas ou obter acesso aos dados e modificá-los de forma fraudulenta;

- **Autoridade de Chave Pública:** também envolve uma terceira parte confiável que teria condições de confirmar se uma chave pública pertence a uma determinada pessoa. Esta confirmação seria feita através da troca de mensagens entre as partes interessadas e a autoridade de chave pública; apesar de ser bastante confiável, este método pode criar problemas relativos ao tráfego excessivo de mensagens;

- **Autoridade Certificadora:** esta abordagem foi sugerida inicialmente por Kohnfelder em [KOH 78] e consiste no uso de certificados que podem ser usados pelas pessoas para anunciar suas chaves públicas sem necessidade de troca constante de

mensagens com a autoridade certificadora; os certificados são criados pela autoridade certificadora que os assina digitalmente e lhes atribui um prazo de validade.

No caso do uso de uma autoridade certificadora, é comum que ela faça parte de uma **ICP** (Infra-Estrutura de Chaves Públicas). Ignaczak [IGN 02] explica que "uma ICP consiste em uma rede de protocolos, padrões e serviços, para suportar aplicações de criptografia de chaves públicas. A ICP define e estabelece a identidade de um usuário para autenticação e autorização".

Não há um único padrão universal para uma ICP mas existem alguns esforços neste sentido. O padrão de certificação X.509 proposto pela organização *Internet Engineering Task Force* é amplamente utilizado e está descrito em inúmeros documentos como em [HOU 02].

No caso da **ICP-Brasil** (Infra-estrutura de Chaves Públicas para o Brasil) existem algumas propostas para um regulamentação de um novo modelo. Algumas delas foram elaboradas no LabSec (Laboratório de Segurança em Computação) da Universidade Federal de Santa Catarina. Este é o caso da dissertação de mestrado de Luciano Ignaczak [IGN 02] onde também pode ser encontrada uma visão geral sobre ICP's. Também pode-se encontrar uma proposta completa de um novo modelo para regulamentação da ICP-Brasil, mais flexível e em conformidade com padrões internacionais foi elaborado pelo professor Ricardo Felipe Custódio em [CUS 01].

4.7 Protocoladora Digital de Documentos Eletrônicos - PDDE

Uma Protocoladora Digital de Documentos Eletrônicos ou PDDE é uma entidade que visa fornecer uma "prova" de que uma determinada informação existiu num dado momento do tempo. O principal papel de uma PDDE é aplicar um "carimbo de tempo" a um dado de modo a comprovar mais tarde que ele efetivamente existiu naquele momento [ADA 01].

As possíveis aplicações para o uso de uma PDDE são incontáveis. Pode

haver necessidade de se verificar que uma assinatura digital foi aplicada a uma mensagem antes da revogação do certificado correspondente. No caso de aplicações onde há uma data limite para submissão de um documento, poderia-se comprovar que tal documento foi submetido dentro do prazo estabelecido. Outra situação ocorre quando um autor deseja provar que seu documento antecedeu a outro similar e, portanto, ele deve deter os direitos sobre o mesmo.

No caso específico deste trabalho, o objetivo do uso de PDDE's está concentrado na comprovação de que um determinado anúncio foi efetivamente publicado na Internet, conforme o contrato feito entre uma **empresa** e um **sítio anunciante**. Isto quer dizer que o **sítio anunciante**, que tenha se comprometido em publicar, por exemplo, um *banner* para a **empresa** que o contratou, pode provar que tal *banner* foi efetivamente publicado e, até mesmo, precisamente em que horário isto ocorreu.

4.7.1 As transações envolvidas no uso de uma PDDE

O artigo [ADA 01] contém informações detalhadas sobre como deve ser um protocolo de datação usando a **Infraestrutura de Chave Pública X.509**. Aqui serão descritas apenas algumas destas informações somente para garantir o mínimo entendimento sobre o funcionamento de uma PDDE.

Para ocorrer uma transação de datação entre um determinado **usuário**[2] e uma **PDDE** os seguintes passos devem ser seguidos (conforme descrito na seção 2.2 de [ADA 01]):

1. **cliente** envia uma requisição de datação para a **PDDE**;
2. **PDDE** responde à requisição do **cliente**;
3. **cliente** faz as seguintes verificações na resposta dada pela **PDDE** para validá-la ou rejeitá-la:
    - verifica o *status* de erro que acompanha a resposta dada pela **PDDE**;

[2]O termo usuário utilizado nesta seção refere-se a qualquer pessoa física ou jurídica interessada nos serviços da PDDE.

- checa a validade da assinatura digital da **PDDE** contida nesta resposta;
- verifica se o “tempo” carimbado na resposta corresponde ao que foi requisitado;
- verifica se a resposta contém o identificador do certificado digital da **PDDE** correto, se o “carimbo de tempo” foi feito sobre os dados desejados e se o algoritmo de *hash* também está correto;
- compara o “carimbo de tempo” aplicado à resposta com uma referência de tempo local confiável; na falta desta referência, pode ser usado um *nonce* (número randômico muito grande com uma alta probabilidade de ser gerado uma única vez pelo **cliente**).

4. **cliente** verifica se certificado digital da **PDDE** não foi revogado (se ainda é válido);
5. **cliente** checa a política de segurança da **PDDE** para determinar se a mesma é adequada para o seu uso.

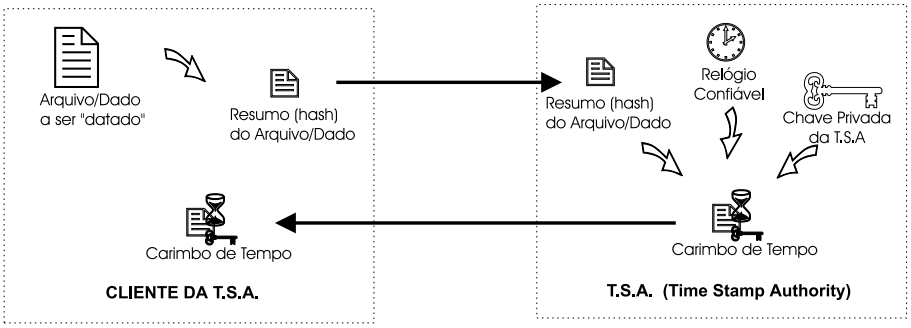


Figura 4.6: Protocoladora Digital de Documentos Eletrônicos (PDDE). A figura mostra um esquema simplificado de transações que envolvem uma Protocoladora Digital de Documentos Eletrônicos (PDDE). O cliente envia um resumo da mensagem a ser datada para a PDDE; ao recebê-lo, a PDDE agrega a ele o “carimbo de tempo” e assina-o digitalmente; em seguida devolve o resultado destas operações (resumo da mensagem datado e assinado) para o cliente.

A figura 4.6 mostra um esquema simplificado das transações envolvidas numa Protocoladora Digital de Documentos Eletrônicos.

É importante salientar que o esquema de datação apresentado é apenas um dentre os inúmeros existentes. Maiores detalhes sobre o tema podem ser encontrados na dissertação de mestrado de Everton Schonardie Pasqual ([PAS 01]) da Universidade Federal de Santa Catarina. Além de descrever diversos mecanismos de datação, Pasqual propõe inclusive uma Infra-Estrutura para Datação de Documentos Eletrônicos.

4.8 Conclusão

Um protocolo criptográfico é uma série de passos, envolvendo duas ou mais partes, projetado para realizar uma tarefa. Os passos são executados, um de cada vez, e nenhum deles pode ser iniciado antes do anterior ter acabado [SCH 96].

Protocolos criptográficos são utilizados para estabelecer comunicação segura em redes abertas e sistemas distribuídos com o objetivo de proporcionar confidencialidade, autenticidade, integridade de dados e não-repúdio, protegendo os objetivos do mesmo em um ambiente hostil [GRI 99]. Assim, o protocolo irá garantir a legitimidade da comunicação.

As técnicas descritas neste capítulo (criptografia simétrica, assimétrica, funções de resumo, assinatura digital, infra-estrutura de chaves públicas e protocoladora digital de documentos eletrônicos) constituem-se na base dos protocolos criptográficos e, portanto, seu conhecimento torna-se essencial para o entendimento do protocolo de que trata este trabalho.

Capítulo 5

Protocolo Criptográfico para Auditoria na Web

5.1 Introdução

Este trabalho apresenta um protocolo criptográfico para auditar e medir a publicidade na Web. Este protocolo baseia-se no uso de cupons eletrônicos que são equivalente digitais aos cupons de desconto usados no mundo real. Estes cupons podem ser obtidos pelos clientes em sítios da Internet e, mais tarde, usados para obter vantagens (brindes ou descontos) na aquisição de bens e serviços. No protocolo aqui proposto, os cupons serão usados como meio de medir a efetividade de anúncios publicados na Internet. Além dos cupons, o protocolo também faz uso de um sistema de auditoria que pode detectar se um sítio anunciante está publicando anúncios de acordo com um contrato estabelecido, bem como medir sua audiência.

A seção 5.2 deste capítulo irá apresentar as características do sistema, incluindo seus requisitos, a base de solução e a notação que será utilizada. A seção 5.3 descreverá o sistema, passo a passo. A seguir, na seção 5.4, serão feitas as considerações sobre a proposta apresentada, tratando-se inclusive do atendimento dos requisitos desejados. Finalmente, a seção 5.5 apresentará conclusões sobre protocolo descrito neste documento.

5.2 Características do Sistema

Uma empresa quer usar a Internet como meio de divulgar seus produtos ou serviços com interesse de incrementar suas vendas e também de fortalecer sua marca tornando-a mais conhecida. Assim como acontece com a escolha de meios de publicidade convencionais, ela irá procurar os sítios de maior popularidade (mais visitados) e, preferencialmente, cujo segmento de mercado seja compatível com seu público-alvo. Para isso, irá contratar uma agência de publicidade que auxiliará na tarefa de escolher o(s) melhor(es) sítio(s) anunciante(s).

5.2.1 Requisitos Básicos do Sistema

O sistema de publicidade aqui proposto possui algumas características desejáveis do ponto de vista de cada participante, como descrito a seguir:

1. **Efetividade para a empresa:** A **empresa** precisa saber se os anúncios publicados atingem os objetivos de divulgação revertendo-se em vendas e/ou contratações de seus produtos/serviços;

2. **Efetividade para a agência de publicidade:** A **agência de publicidade** também precisa receber a informação sobre a efetividade dos anúncios publicados num **sítio anunciante** pois seu objetivo é indicar para a **empresa** os melhores locais para exibir seus anúncios; a fidelidade desta informação implica diretamente na confiabilidade da **agência de publicidade** perante a **empresa**;

3. **Efetividade para o sítio anunciante:** O **sítio anunciante** também precisa saber o grau de efetividade dos anúncios publicados de modo a poder medir o quanto pode cobrar pelo seu espaço de anúncio em contratos futuros de publicidade;

4. **Vantagem para o cliente:** Do ponto de vista do **cliente**, o objetivo é encontrar os produtos/serviços que lhe ofereçam as melhores vantagens;

5. **Auditoria do contrato de publicidade:** Outra característica importante do ponto de vista da **empresa** e também da **agência de publicidade** é a garantia de que o

contrato com o **sítio anunciante** esteja sendo cumprido, isto é, que o anúncio esteja sendo publicado com a freqüência e durante o tempo que foi contratado;

6. **Medição da audiência:** O **sítio anunciante** tem interesse em comprovar sua audiência de modo a valorizar a oferta pelo seu espaço de publicidade;

7. **Privacidade do cliente:** Os dados pessoais do **cliente** não devem ser publicados em nenhum momento durante a execução das etapas do protocolo;

8. **Proteção dos participantes:** O protocolo deve proteger todos os participantes envolvidos (**empresa**, **agência de publicidade**, **sítio anunciante** e **cliente**) de qualquer fraude que possa ser originada por outro participante ou mesmo de um oponente externo.

5.2.2 Solução proposta

Para satisfazer os requisitos do sistema anteriormente enumerados, o protocolo fará uso de cupons eletrônicos e de um sistema de auditoria de publicidade. Será demonstrado que proposta de cupons eletrônicos oferece solução para os quatro primeiros requisitos citados. Para garantir o quinto e o sexto requisitos será usada uma terceira parte confiável que será responsável pela auditoria do sítio anunciante e da empresa. Os dois últimos requisitos serão garantidos através da forma como o protocolo funcionará, tal como será demonstrado adiante.

A proposta de cupons eletrônicos para medição de publicidade foi apresentada inicialmente em [JAK 99]. Algumas outras propostas também fundamentaram-se neste mesmo tema como em [CIM 01], [GAR 01] e [BLU 02]. Como já foi descrito no capítulo 3, nenhuma destas propostas contempla todos os requisitos aqui apresentados.

A medição da efetividade dos anúncios a partir de cupons eletrônicos fundamenta-se na idéia de que a empresa, ao receber o cupom (que foi emitido por ela mesma) de um cliente no ato de uma compra, saberá que este cliente foi atingido pela campanha publicitária. Saberá também a partir de onde este cupom foi obtido, o que lhe dará a informação dos sítios mais adequados para suas próximas campanhas publicitárias.

Porém, a efetividade dos anúncios não abrange todos os aspectos de medição em uma campanha publicitária. Um aspecto que não é resolvido com os cupons eletrônicos é o da necessidade de saber se o sítio anunciante está publicando os anúncios conforme contratado. Caso isto seja verdade, há ainda a questão da medição da audiência do sítio. Para a empresa é tão importante saber se seus anúncios estão sendo veiculados quanto se o sítio é freqüentemente visitado de forma que os anúncios estejam chegando até seu público-alvo. Os cupons não dão prova desta medida pois um sítio pode distribuir inúmeros cupons a clientes e o visitam e, no entanto, é possível que estes clientes jamais venham a utilizar estes cupons. Deste modo, a empresa não ficará sabendo que estes clientes foram atingidos pela campanha, ou seja, que o sítio anunciante está cumprindo o seu papel. Outro aspecto relevante é: como é a empresa que recebe os cupons para serem resgatados, que meios seriam usados para garantir que ela revelará corretamente a quantidade de cupons resgatados?

Para resolver estas questões o protocolo aqui descrito fará uso de um Sistema de Auditoria que irá acompanhar tanto a distribuição de cupons feita pelo sítio anunciante quanto o resgate deles quando são devolvidos à empresa por um cliente.

5.2.3 Notação

Para especificar o protocolo será usada a seguinte notação:

- **EM - Empresa:** diz respeito à empresa que tem interesse em anunciar seus produtos e serviços na Internet; é a “parte” interessada em anunciar;
- **AP - Agência de Publicidade:** entidade que é contratada pela empresa para viabilizar o anúncio de seus produtos e serviços. Na maioria dos casos este papel é representado por uma empresa distinta especializada em publicidade; porém, algumas vezes, pode ser assumido por um departamento da própria empresa que pretende anunciar seus produtos/serviços;
- **SA - Sítio Anunciante:** portal da Internet onde os anúncios serão publicados. Dependendo da estratégia escolhida pela agência de publicidade, podem ser inúmeros

os sítios escolhidos para divulgação;

- **CL - Cliente:** refere-se ao usuário da Internet que é alvo da empresa como potencial comprador;

- **PD - Protocoladora Digital de Documentos Eletrônicos:** agente confiável que possui recursos para estampar um carimbo de tempo em um documento eletrônico;

- **AU - Sistema de Auditoria:** agente confiável responsável pela auditoria do sítio anunciante para garantir que os anúncios estejam sendo publicados conforme o contrato estabelecido previamente;

- **EC - E-Cupom:** documento eletrônico equivalente aos cupons de desconto usados no "mundo real" que permitem aos cliente obter vantagens (descontos, brindes) na aquisição de produtos ou serviços da empresa que os emitiu;

- **C - Cifrar:** ato de cifrar uma mensagem digital usando uma chave (senha);

- **D - Decifrar:** ato de decodificar uma mensagem previamente cifrada fazendo uso de uma chave que pode ser ou não a mesma chave usada no processo de cifragem;

- **A - Assinatura Digital:** função aplicada a uma mensagem para garantir a autenticidade de seu emissor; é o equivalente eletrônico das assinaturas em papel;

- **CT - Carimbo de Tempo:** ato de protocolar digitalmente uma mensagem eletrônica para garantir que ele existiu num dado momento do tempo.

A representação formal das mensagens repassadas a cada etapa do protocolo, e que aparece abaixo da descrição destas etapas, foi feita com base em Menezes [MEN 96] conforme no exemplo a seguir:

$$EM \rightarrow AP : M$$

que significa que EM envia a mensagem M para AP.

5.3 Descrição do Sistema

Para dar início ao sistema de publicidade de que trata este protocolo são necessárias algumas etapas iniciais que irão estabelecer o contrato entre algumas das partes. Estas etapas podem acontecer sem a necessidade de transações eletrônicas e estão descritas a seguir:

- O sistema inicia com um contrato de publicação de anúncios baseado no uso de cupons eletrônicos que é firmado entre a **empresa** e a **agência de publicidade**;
- A seguir, a **agência de publicidade** irá escolher o(s) **sítio(s) anunciante(s)** que irá(ão) publicar o anúncio e com o(s) qual(is) também firmará um contrato de publicidade;
- Após isso, a tanto a **agência de publicidade** quanto a **empresa** poderão negociar com o **Sistema de Auditoria** para que seja responsável pela medição de publicação de anúncios junto ao **sítio anunciante** e junto à **empresa**.

Efetuados estes contratos, o sistema passa a funcionar através das transações eletrônicas seguras descritas a seguir e ilustradas na figura 5.1:

1. A **agência de publicidade** solicita à **empresa** que crie um cupom eletrônico para um determinado **sítio anunciante**.

$$AP \rightarrow EM : Req\_Novo\_EC$$

onde

$Req\_Novo\_EC = A_{AP}(ID_{SA})$

ID_{SA} = identificação do **sítio anunciante** e

A_{AP} = significa que a mensagem será assinada digitalmente pela **agência publicidade** para garantir que foi realmente emitida por ela.

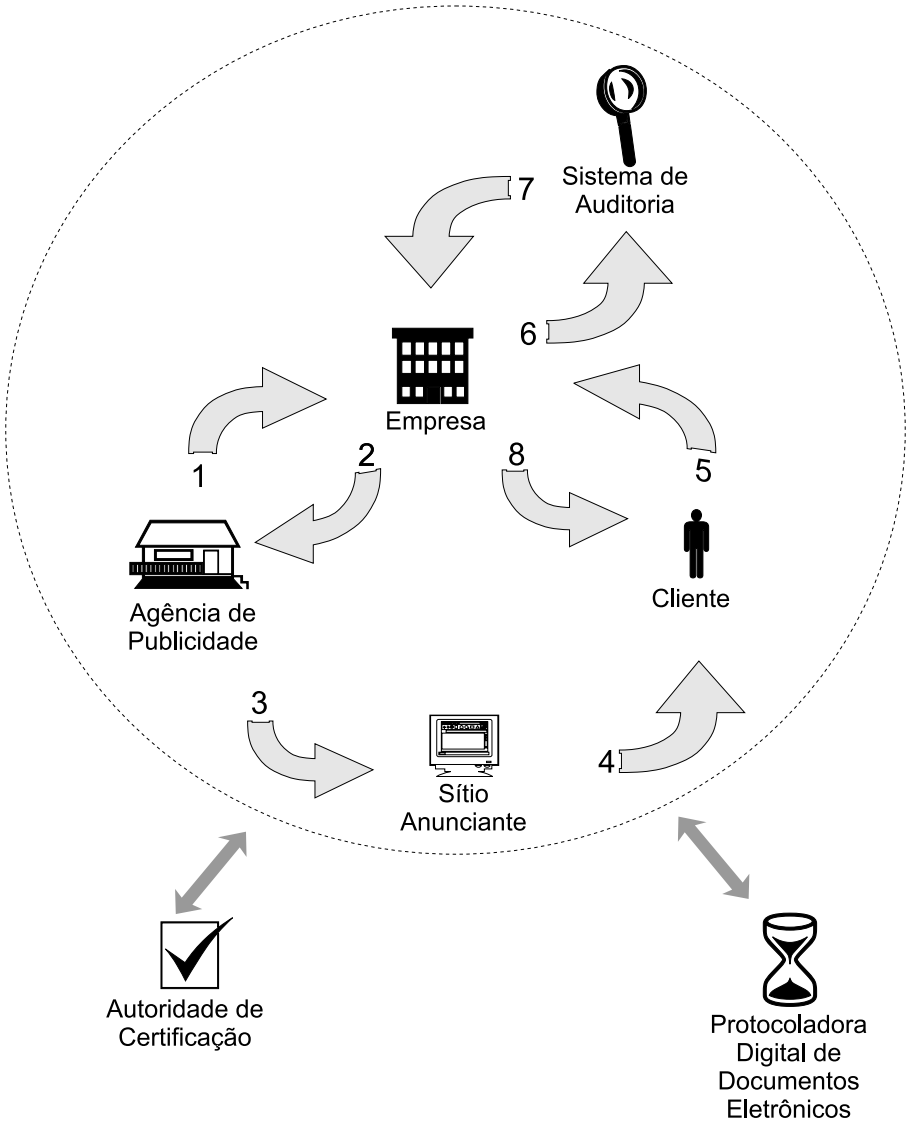


Figura 5.1: Esquema simplificado do protocolo proposto. Após a requisição do cupom (1) feita pela Agência de Publicidade o cupom é gerado (2) pela Empresa e repassado (3) ao Sítio Anunciante; quando um Cliente visita o Sítio Anunciante ele pode ganhar um cupom (4) e, mais tarde, resgatá-lo (5) junto à Empresa; no momento do resgate a Empresa repassa o cupom para o Sistema de Auditoria (6) que irá decifrá-lo e devolvê-lo (7) para Empresa. Esta, por sua vez, poderá oferecer ao cliente (8) os benefícios que o cupom lhe dá direito.

2. A **empresa**, atendendo a solicitação da **agência de publicidade**, cria o cupom eletrônico contendo um texto descritivo da promoção que está sendo realizada e mais um código identificador do **sítio anunciante**. Este cupom eletrônico é assinado digitalmente com a chave privada da **empresa**, recebe o "carimbo de tempo"[1] de uma protocoladora digital de documentos eletrônicos e é enviado à **agência de publicidade** que o solicitou.

$$EM \rightarrow AP : EC_{EM}$$

onde

$EC_{EM} = A_{EM}(ID_{SA}, TXT, V, CT)$ = cupom emitido pela **empresa**

ID_{SA} = identificação do **sítio anunciante** e

TXT = texto descritivo do cupom eletrônico que identifica o tipo de promoção que está sendo oferecida e a qual benefício ele dará direito

V = indica o prazo de validade do cupom e pode conter inclusive hora, minuto, segundo, etc.

CT = significa que o cupom receberá um carimbo de tempo da Protocoladora Digital de Documentos Eletrônicos confirmando o instante em que foi criado

A_{EM} = significa que a mensagem será assinada digitalmente pela **empresa** para garantir que foi realmente emitida por ela.

3. A **agência de publicidade** recebe o cupom, assina-o também com sua chave privada e repassa-o ao **sítio anunciante**. Esta assinatura poderá, mais tarde, comprovar que o **sítio anunciante** foi recomendado por ela, e não por outra agência concorrente que pode ter sido, eventualmente, contratada para auxiliar na publicação do mesmo anúncio e mesmo cupom.

[1] Este carimbo de tempo poderá dar provas futuras de que, quando o cupom foi emitido, a assinatura digital da **empresa** era válida quando ele foi criado. Esta característica irá proteger o **cliente** caso o certificado digital da **empresa** seja revogado antes que ele tente resgatar o cupom.

$$AP \rightarrow SA : EC(_{AP,EM})$$

onde

$EC(_{AP,EM})$ = $A_{AP}(EC_{EM})$ = Cupom eletrônico recebido da **empresa** e assinado digitalmente pela **agência de publicidade** para ser repassado ao **sítio anunciante**.

$EC_{EM} = A_{EM}(ID_{SA}, TXT, V, CT)$ = cupom emitido pela **empresa** e cujos detalhes já estão descritos na etapa anterior

A_{AP} = significa que a mensagem será assinada digitalmente pela **agência de publicidade** para garantir que foi realmente emitida por ela.

4. O **cliente**, ao visitar o **sítio anunciante**, vê o anúncio publicado e, caso aceite, recebe o cupom eletrônico que lhe dará direito a algum benefício posteriormente; no momento da entrega ao **cliente**, o cupom recebe um novo "carimbo de tempo", registrando assim o instante exato em que o **cliente** recebeu este documento eletrônico. Neste instante, o cupom é cifrado com a chave pública do **Sistema de Auditoria** de modo que, mais tarde, só possa ser aberto com a participação deste.

$$SA \rightarrow CL : EC$$

onde

$EC = C_{AU}(EC_{AP,EM}, CT)$ = Cupom eletrônico recebido da **agência de publicidade**, originado pela **empresa**, protocolado digitalmente com um "carimbo de tempo" e cifrado com a chave pública do **Sistema de Auditoria**

5. O **cliente**, opcionalmente, pode resgatar o cupom enviando-o para a **empresa** de modo a trocá-lo por algum benefício.

$$CL \rightarrow EM : EC$$

onde

EC = Cupom eletrônico repassado ao **cliente** pelo **sítio anunciante**

6. Neste momento, a **empresa** terá que repassar o cupom para o **Sistema de Auditoria** para que ele decifre[2] o conteúdo do cupom.

$$EM \rightarrow AU : EC$$

onde

EC = Cupom eletrônico repassado ao **cliente** pelo **sítio anunciante**

7. O **Sistema de Auditoria**, após abrir o cupom com sua chave privada, devolve o conteúdo para a **empresa**. De posse do cupom decifrado, a **empresa** terá condições de checar a validade[3] do cupom e, com isso, oferecer o benefício ao **cliente**. O cupom resgatado poderá ser armazenado num banco de dados da **empresa** para garantir que ele, caso o **cliente** tente utilizá-lo novamente, seja rejeitado. Neste momento em que é gravado no banco de dados, o cupom recebe novo "carimbo de tempo" que comprova o momento de seu resgate.

$$AU \rightarrow EM : C_{EM}(EC)$$

onde

EC = Cupom eletrônico repassado ao **cliente** pelo **sítio anunciante**

C_{EM} = Ato de cifrar o cupom eletrônico com a chave pública da **empresa** de modo que somente ela possa abrir seu conteúdo.

8. A **empresa** pode fornecer ao **cliente** os benefícios que o cupom lhe garante. Esta etapa estará geralmente condicionada a um contrato de compra e venda de produtos ou serviços entre ambas as partes. Os detalhes deste procedimento não são objetos de estudo deste protocolo.

[2] A participação do **Sistema de Auditoria** no processo de resgate do cupom irá garantir aos outros participantes que houve uma tentativa de resgate do cupom

[3] A validade do cupom que pode ser verificada pela **empresa** diz respeito tanto à checagem da data de prazo (que pode ter sido estipulada pela empresa) quanto às assinaturas digitais contidas no cupom.

9. O **Sistema de Auditoria** pode fornecer informações referentes à publicação dos anúncios, indicando se eles foram publicados pelo **sítio anunciante** conforme combinado previamente no contrato. Além disso, fornece informações sobre a audiência do **sítio anunciante** e sobre os resgates de cupons junto à **empresa**. A figura 5.2 ilustra as interações do **Sistema de Auditoria** com os demais participantes. Estas auditorias podem ser feitas com o auxílio de uma **Protocoladora Digital de Documentos Eletrônicos** da seguinte forma:

   (a) O **Sistema de Auditoria**, fiscaliza a publicação dos anúncios no **sítio anunciante** através de seus arquivos de log, usando técnicas como funções de resumo e protocolização digital de documentos eletrônicos para garantir a confiabilidade das informações fornecidas. Para reforçar a segurança das informações, o **Sistema de Auditoria** pode também acessar[4] o **sítio anunciante** e obter cupons eletrônicos como se fosse um **cliente**. Isto lhe permitirá, mais tarde, confrontar as informações geradas na etapa anterior pois estes acessos deverão estar corretamente registrados naqueles arquivos. O cupom recebido pelo **Sistema de Auditoria** é datado com um "carimbo de tempo", tal como ocorre quando um cupom é remetido a um **cliente**;

   (b) Através do mesmo mecanismo de usado para fiscalizar a publicação dos anúncios, o **Sistema de Auditoria** poderá fornecer informações referentes à medição de audiência sítio.

   (c) O **Sistema de Auditoria**, fiscaliza os cupons resgatados por **clientes** junto à **empresa** através de seus arquivos de log, usando técnicas como funções de resumo e protocolização digital de documentos eletrônicos tal como acontece com a fiscalização dos **sítios anunciantes**. No momento do resgate do cupom, a **empresa** tem que repassar o cupom para o **Sistema de Auditoria** para que ele o abra, ou seja, para que o decifre. Além de poder confrontar os dados referentes ao resgate de cupom com a etapa anterior, o **Sistema de Auditoria** poderá informar aos outros participantes a quantidade cupons que tentaram

[4] O acesso ao **sítio anunciante** pode ser feito em momentos pré-determinados ou esporadicamente

ser resgatados por **clientes** de modo a confirmar (ou não) as informações de efetividade fornecidas pela **empresa**. Para aumentar o grau de confiabilidade destas informações, o **Sistema de Auditoria** pode fazer uso de um PDDE para adicionar um "carimbo de tempo" ao cupom recebido confirmando seu resgate (ou a tentativa de) naquele instante do tempo. Vale salientar que, o número de cupons que passarão pelo **Sistema de Auditoria** para serem resgatados pode não ser igual ao número de cupons revertidos em vendas para a **empresa**. Isto pode acontecer porque o cupom é repassado ao **Sistema de Auditoria** antes do cliente confirmar a compra. Toda vez que o processo de compra não se confirmar, seja porque o **cliente** desistiu da compra, seja porque houve falha de comunicação ou mesmo porque a **empresa**, por qualquer motivo, não tenha aceito o cupom.

(d) O **Sistema de Auditoria** poderá enviar as informações referentes às operações de entrega e resgate de cupons bem como da audiência do sítio, para quaisquer dos três participantes: **empresa**, **agência de publicidade** e **sítio anunciante**.

5.4 Considerações Sobre a Proposta

Para a compreensão da proposta descrita neste trabalho, é prudente que sejam feitas algumas considerações acerca de seu funcionamento. A seguir será descrito como o sistema atende aos requisitos de segurança bem como àqueles propostos na seção 5.2.1.

5.4.1 Atendimento dos Requisitos Básicos do Sistema

O sistema proposto atende aos requisitos previamente estabelecidos (seção 5.2.1) conforme descrito a seguir:

1. **Efetividade para a empresa:** A medição da efetividade dos anúncios é garantida através dos cupons eletrônicos resgatados pelos clientes. O número de cupons

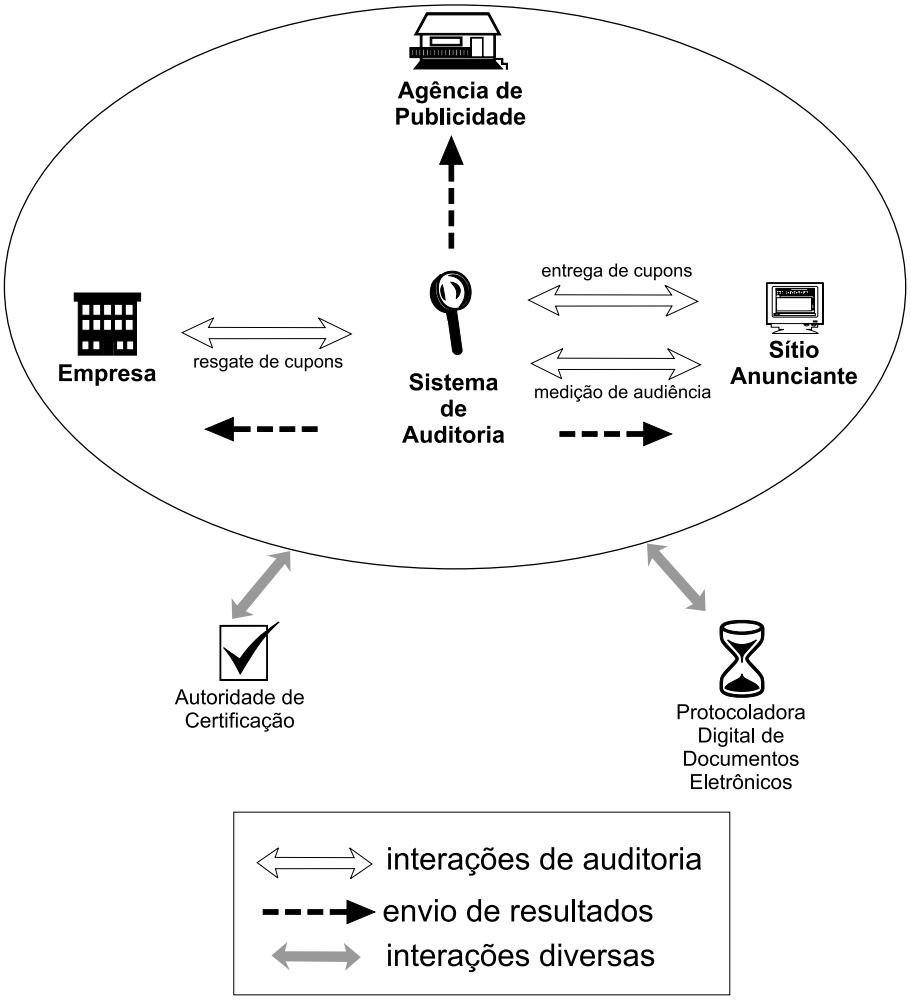


Figura 5.2: Interações do Sistema de Auditoria. A figura mostra as interações do **Sistema de Auditoria** com os demais participantes: a **empresa** e o **sítio anunciante** são auditados em três diferentes situações; a **empresa**, o **sítio anunciante** e a **agência de publicidade** recebem os resultados destas auditorias.

resgatados equivale diretamente ao número de clientes atingidos pela campanha indicando inclusive o sítio anunciante em que foram publicados e a **agência de publicidade** que o selecionou. Estas informações estão contidas nos cupons.

2. **Efetividade para a agência de publicidade:** O **Sistema de Auditoria**, que tem o controle sobre os cupons que chegam até a **empresa** para serem resgatados, repassa esta informação para a **agência de publicidade**. Embora nem todos os cupons que chegam ao **Sistema de Auditoria** tenham sido necessariamente convertidos em vendas para a **empresa**, do ponto de vista da **agência de publicidade** é possível considerar que o anúncio foi ´´efetivo" pois comprova que o **cliente** visitou o **sítio anaunciante** que foi indicado por ela;

3. **Efetividade para o sítio anunciante:** Exatamente do mesmo modo como acontece com a **agência de publicidade**, o **sítio anunciante** recebe as informações do **Sistema de Auditoria** e pode constatar quantos dos cupons emitidos por ele chegaram até a **empresa**;

4. **Vantagem para o cliente:** A proposta de cupons eletrônicos traz vantagens diretas para o **cliente** já que o objetivo dos cupons é o de oferecer algum tipo de promoção de forma a atrair o **cliente** e levá-lo a adquirir bens ou serviços de uma determinada **empresa**; ao navegar na Internet o **cliente** irá procurar sempre a oferta que lhe trouxer maior vantagem;

5. **Auditoria do contrato de publicidade:** A garantia de que o contrato com o **sítio anunciante** está sendo cumprido é fornecida pelo **Sistema de Auditoria** que terá condições de informar, tanto a **empresa** quanto a **agência de publicidade** se o anúncio está sendo publicado com a freqüência e durante o tempo que foi contratado;

6. **Medição da audiência:** Através do mesmo processo de fiscalização que permite ao **Sistema de Auditoria** controlar a publicação dos anúncios, ele fará a medição de audiência do **sítio anunciante**;

7. **Privacidade para o cliente:** Os dados pessoais do **cliente** não serão publicados em nenhum momento durante a execução das etapas do protocolo e nem sequer serão solicitados[5]

8. **Proteção dos participantes:** O tratamento deste requisito será detalhado na seção 5.4.3 onde estes aspectos de segurança do protocolo serão tratados.

5.4.2 Características de Segurança

O protocolo criptográfico apresentado atende aos seguintes requisitos de segurança:

- **Cupons Falsos**: as assinaturas digitais que acompanham o cupom eletrônico inviabilizam sua falsificação. Para que um participante mal intencionado ou mesmo qualquer elemento externo ao sistema crie um cupom falso, seria necessário primeiramente, conhecer a chave privada da empresa e além disso, a chave privada da agência de publicidade pois esta seria a única maneira de gerar cupons que poderiam ser aceitos como válidos.

- **Validade dos Cupons**: embora esta característica não seja relevante para o protocolo em questão, pode ser relevante para a **empresa** o fato de que os cupons tenham uma data de validade. Assim, ela pode estipular um prazo dentro do qual a promoção dos cupons distribuídos é válida e, com isso, rejeitar cupons que tentem ser resgatados fora deste prazo.

- **Rejeição de cupons**: a geração de um cupom envolve a assinatura digital da **empresa**. Desta forma, pode ocorrer a revogação do certificado digital durante o tempo

[5]Quando o cliente fizer o resgate do cupom ele deverá efetuar alguma compra ou contratação perante a empresa. Este processo de compra deve possivelmente exigir a identificação do cliente como ocorre normalmente em transações de comércio eletrônico. Este evento, porém, não faz parte do escopo deste protocolo. No protocolo aqui proposto, seria possível que o cupom fosse adquirido por um cliente e repassado para outro que poderia usufruir dos benefícios normalmente já que o cupom não carrega nenhuma identificação do cliente.

de “vida” do cupom (desde que foi criado pela **empresa** até o momento de ser resgatado pelo **cliente**). Neste caso, o **cliente** ainda terá direito a resgatar o cupom pois o “carimbo de tempo” que indica a criação do cupom indicará que naquele momento em que ele foi gerado, o certificado digital ainda era válido e, portanto, o cupom é autêntico e deve ser aceito. Caso ocorra a situação contrária, ou seja, se o cupom que tentar ser resgatado tiver sido criado após a data de revogação do certificado digital, ele poderá ser rejeitado pela **empresa** pois deve tratar-se de uma fraude. Aqui, um ponto relevante deve ser considerado: para manter sua imagem perante os clientes, a **empresa** pode optar por aceitar cupons “inválidos” do ponto de vista da autenticidade eletrônica. Outra característica importante é o fato de que, ainda que um cupom tenha sido detectado como forjado, a opção por aceitá-lo deve implicar numa nova venda ou contratação, que é o grande objetivo da **empresa** num sistema de publicidade. Assim, a decisão de aceitar cupons “inválidos” pode fazer parte da política da empresa e não é alvo de estudo deste trabalho.

- **Unicidade de cupons**: apesar de não conterem um número identificador que poderia ser usado como “chave” para distingüir os cupons entre si, é possível garantir a não duplicidade deles. Revendo a trajetória de um cupom, observa-se que a **empresa** cria, na verdade, uma espécie de “cupom-raiz” pois, a partir deste documento único é que o **sítio anunciante** irá gerar os cupons a serem distribuídos aos **clientes**. No momento em que o **sítio anunciante** repassa o cupom ao **cliente**, ele recebe um outro “carimbo de tempo”. Desta forma, quando chega ao **cliente**, o cupom passa a ter uma identificação única, pois além de conter um identificador **sítio anunciante** que o distribuiu, ele carrega a comprovação inequívoca do instante em que foi recebido.

- **Tentativa de resgate de cupom já utilizado**: no momento do resgate do cupom, a **empresa** irá armazená-lo em um banco de dados pessoal. Assim, a cada novo pedido de resgate de cupom, este banco de dados será consultado para verificar se o cupom já foi utilizado. Se for o caso, a **empresa** poderá rejeitar o cupom. Como o cupom passa pelo **Sistema de Auditoria** para ser decifrado, este também mantém

o controle dos cupons resgatados e pode confirmar (ou não) a tentativa de resgate repetida de um mesmo cupom. Como já foi descrito no item que trata da rejeição de cupons, pode não ser interessante para a **empresa** rejeitar um cupom, ainda que ela detecte que ele não é válido. Um fator agravante no caso da tentativa de resgate do mesmo cupom é que não há nenhum vínculo com o **cliente** que o obteve, isto é, o cupom é uma espécie de "documento eletrônico ao portador". Isto significa que, se algum intruso conseguir obter um cupom que foi recebido por um **cliente** e fizer uma cópia para si, ele poderá usá-lo até mesmo antes do próprio dono do cupom original.

5.4.3 Considerações sobre Ataques Possíveis

Um protocolo envolve uma série de mensagens que são trocadas entre as partes integrantes do sistema. O tráfego destas informações pode estar vulnerável a diversos tipos de ataques (já descritos no capítulo 4). Nesta seção serão feitas algumas considerações que comprovam a segurança do protocolo sob o ponto de vista de cada mensagem enviada.

1. A **agência de publicidade** solicita à **empresa** que crie um cupom eletrônico para um determinado **sítio anunciante**.

$$AP \rightarrow EM : Req\_Novo\_EC$$

Um oponente mal intencionado poderia tentar fabricar esta requisição em nome da **agência de publicidade**. Isto, porém, seria detectado pois a requisição é assinada digitalmente pela agência não podendo, desta forma, ser emitida por um terceiro. Se, por outro lado, o oponente capturasse a mensagem e tentasse, mais tarde, reenviar a solicitação para a **empresa** criando uma duplicidade da mensagem, a **empresa** imediatamente detectaria a fraude pois já teria recebido a mesma mensagem da **agência de publicidade**e não haveria sentido em recebê-la de novo e recriar os cupons-raiz para o mesmo **sítio anunciante** e para a mesma campanha publicitária.

De outra forma, caso o oponente interceptasse a mensagem e tentasse modificá-la, isto seria detectado pois as técnicas de assinaturas digitais garantem a autenticidade da mensagem.

2. A **empresa** cria o cupom eletrônico contendo um texto descritivo da promoção que está sendo realizada e mais um código identificador do **sítio anunciante** e envia-o para a **agência de publicidade**.

$$EM \rightarrow AP : A_{EM}(EC_{EM}, CT)$$

Do mesmo modo como acontece com a mensagem anterior, o cupom-raiz enviado pela empresa é assinado digitalmente por ela. Além disso, recebe o carimbo de tempo da PDDE. O processo de protocolização digital de documentos eletrônicos é padronizado e aceito por todos os participantes como confiável. Por estes motivos, ataques de fabricação ou modificação seriam imediatamente detectados. Se um oponente interceptar a mensagem e copiá-la para si, ele não poderá usá-la pois ela contém a identificação do **sítio anunciante** e além disso não irá conter a assinatura da **agência de publicidade** homologada pela **empresa**.

3. A **agência de publicidade** assina o cupom recebido e repassa-o ao **sítio anunciante**.

$$AP \rightarrow SA : EC(_{AP,EM})$$

Seguindo a mesma lógica das mensagens analisadas anteriormente, a assinatura digital da **agência de publicidade** garante a autenticidade da mensagem que não poderia, assim, ser fabricada ou modificada por um oponente. Também não haverá vantagens para este oponente em manter uma cópia desta mensagem para usá-la pois ela ainda não constitui-se em um cupom. Seria necessário a intervenção da PDDE e do **Sistema de Auditoria** para transformá-la num cupom útil.

4. O **cliente**, ao visitar o **sítio anunciante**, recebe o cupom eletrônico que lhe dará direito a algum benefício posteriormente;

$$SA \rightarrow CL : EC$$

Neste momento de entrega do cupom ao **cliente**, faz-se uso de uma PDDE e do **Sistema de Auditoria**. Seria possível, no entanto, que um oponente interceptasse esta mensagem quando ela estivesse sendo transmitida ao cliente e fizesse inúmeras cópias dela, criando réplicas do cupom eletrônico do **cliente**. Além disso, este oponente poderia resgatar estes cupons replicados antes mesmo do **cliente** que possui o cupom original já que no caso de documentos eletrônicos não há diferenças entre original e cópia. A fraude porém, seria detectada. O tratamento desta situação já foi exposto no item que trata da tentativa de resgate do mesmo cupom, na seção 5.4.2 que trata das características de segurança.

5. O **cliente** resgata o cupom enviando-o para a **empresa** de modo a trocá-lo por algum benefício.

$$CL \rightarrow EM : EC$$

Identicamente à descrição do item anterior, caso o cupom seja interceptado por um oponente e copiado, ele poderia ser resgatado apesar de que a fraude seria detectada.

6. A **empresa** repassa o cupom para o **Sistema de Auditoria** para que ele decifre o conteúdo do cupom.

$$EM \rightarrow AU : EC$$

Como o processo de decifragem prevê o uso da chave privada do **Sistema de Auditoria**, ninguém mais estaria apto a realizar esta tarefa.

7. O **Sistema de Auditoria** abre o cupom com sua chave privada e devolve o conteúdo para a **empresa**.

$$AU \rightarrow EM : C_{EM}(EC)$$

Ainda que a mensagem acima seja interceptada e copiada por um oponente, para obter os benefícios do cupom ele terá que efetuar alguma compra ou contratação com a **empresa** de modo a usufruir das vantagens, o que pode ser vantajoso para a **empresa**, mesmo sabendo sobre a fraude.

8. A **empresa** fornece ao **cliente** os benefícios que o cupom lhe garante.

   Do mesmo modo como no item anterior, como as vantagens do cupom estão atreladas a compras e contratações, estes benefícios serão direcionados exclusivamente para o cliente que estiver realizando a compra e não poderá ser repassado a terceiros.

5.4.4 Comportamento Malicioso

Nesta seção serão apresentadas as considerações sobre possíveis comportamentos maliciosos dos participantes do protocolo:

- **Empresa:** a empresa poderia agir em benefício próprio quando não informar corretamente quantos dos cupons que tentaram ser resgatados converteram-se em vendas. A vantagem obtida seria uma possível tentativa de desvalorização do sítio anunciante ou da agência de publicidade num próximo contrato de publicidade, alegando que sua campanha não atingiu níveis adequados. Para evitar este problema, o Sistema de Auditoria mantém o controle sobre os cupons que tentaram ser resgatados pois ele tem que decifrá-los e faz a auditoria dos arquivos de log de modo a fazer o cruzamento destas informações e a checagem de sua veracidade.

- **Agência de Publicidade:** a agência de publicidade, com o objetivo de provar que os sítios anunciantes recomendados por ela são eficientes (e conseqüentemente ela também o é por tê-los recomendado), pode tentar forjar a audiência destes sítios mediante a visita freqüente nos mesmos com a premeditada obtenção de cupons que na verdade nunca serão resgatados. Com isso poderia alegar que o sítio está fazendo sua parte mesmo que os cupons não estejam sendo revertidos em vendas. Este comportamento mal-intencionado por parte da agência de publicidade poderia ser detectado pelo Sistema de Auditoria através dos arquivos de log que denunciariam

a origem das mensagens e poderiam detectar a fraude. Ainda que não detectasse, a empresa, cujo interesse é converter seus anúncios em vendas, poderia simplesmente não renovar o contrato com a agência pelo simples fato de não alcançar seu objetivo maior.

- **Sítio Anunciante:** o sítio anunciante pode agir de má-fé com o objetivo de provar altos índices de audiência e grande número de cupons distribuídos. Neste caso, poderá adotar um comportamento idêntico ao descrito anteriormente para a agência de publicidade. As mesmas formas de detecção de fraude descritas para aquele caso, aplicam-se ao sítio anunciante.

- **Cliente:** o cliente visa obter as maiores vantagens possíveis no momento da aquisição de um bem ou serviço. Por este motivo, seu comportamento malicioso poderia ser a tentativa de resgate do mesmo cupom duplamente. Porém, como a empresa mantém uma base de dados dos cupons resgatados que contém dados relativos à compra que permitiu o uso do benefício do cupom, ela poderá facilmente identificar se o cliente que está tentando usar o cupom é o mesmo que o utilizou anteriormente. Conforme já foi dito, a empresa terá vantagens em aceitar o cupom novamente se assim o desejar ou poderá rejeitá-lo se quiser. Neste último caso, poderá contar com a ajuda do Sistema de Auditoria que também mantém controle sobre cupons resgatados.

5.5 Conclusão

Neste capítulo foi apresentado o protocolo criptográfico para auditoria da publicidade na Web. Este protocolo faz uso de cupons eletrônicos para medir a efetividade dos anúncios e utiliza um Sistema de Auditoria para verificar o cumprimento adequado do contrato de publicação dos anúncios bem como medir a audiência do sítio anunciante e controlar o resgate de cupons pelos clientes junto à empresa.

Apesar de existirem algumas propostas do uso de cupons eletrônicos como em [JAK 99], [CIM 01], [GAR 01] e [BLU 02], o protocolo aqui proposto traz

algumas inovações. Uma destas inovações trata-se da inclusão de um novo participante: a **agência de publicidade**. Esta inclusão foi feita com base nos estudos sobre publicidade e propaganda pois, num modelo convencional de publicação de anúncios, há sempre um agente responsável pela contratação dos veículos anunciantes e que, na maioria das vezes, também cria a propaganda a ser veiculada, além de poder acumular outras atividades menos importantes para o sistema aqui proposto.

Outra inovação diz respeito ao uso de uma **Protocoladora Digital de Documentos Eletrônicos** para autenticar os cupons com "carimbos de tempo" (tanto na criação quanto na entrega ao **cliente** e mesmo no resgate dos benefícios). Esta característica irá adicionar maior confiabilidade ao sistema pois a comprovação da existência deste "documento eletrônico" em diferentes momento de sua trajetória será, teoricamente, incontestável[6].

Outra característica desta proposta é a auditoria da publicação dos anúncios, aqui apresentada como "Sistema de Auditoria de Publicidade", ou seja, o trabalho aqui descrito preocupa-se também com a garantia de que os anúncios solicitados sejam efetivamente publicados conforme acordo prévio.

Mais uma contribuição importante da proposta aqui apresentada é o fato de garantir a confiabilidade do sistema a todos os participantes, sem exceção. A maioria das propostas existentes parte do princípio que uma das partes (geralmente a empresa) é a maior interessada do sistema e, por isso, ela é honesta. Se apenas a empresa puder ter o controle de quantos cupons chegaram até ela e foram revertidos em vendas, como garantir que ela repassará esta informação corretamente? O protocolo aqui proposto apresentou uma sugestão de como este conflito pode ser resolvido.

Com relação ao método de auditoria através da instalação de um software no servidor do auditado, gerando arquivos de resumo em tempos aleatórios, há um trabalho similar feito pelo IVC - Instituto Verificador de Circulação e apresentado no documento [dMI 00].

[6] A expressão "teoricamente incontestável" foi aqui utilizada apenas porque, na verdade, a autenticidade de um documento "eletronicamente datado" está diretamente ligado à confiabilidade da Protocoladora Digital de Documentos Eletrônicos escolhida, tal como acontece com as Autoridades Certificadoras.

Os requisitos propostos foram atendidos e a possiblidade de ataques à segurança do sistema foi analisado do ponto de vista de cada participante e também de um oponente externo.

A implementação simplificada do protocolo foi produzida por alunos de graduação do curso de Ciência da Computação num projeto diretamente integrado com a dissertação de mestrado aqui apresentada. Esta implementação será descrita com detalhes mais adiante.

Capítulo 6

Implementação do Sistema

A proposta contida nesta dissertação de mestrado motivou a criação de um projeto para implementar o protocolo criptográfico para auditoria na Web. O projeto foi desenvolvido pelos alunos de graduação do curso de Bacharelado em Ciência da Computação da Universidade Federal de Santa Catarina, Fernando Karl e Geovane Pasa, na forma de seu Trabalho de Conclusão de Curso.

Para facilitar a implementação foi criado um modelo simplificado do protocolo aqui proposto, cujas limitações serão aqui detalhadas.

A seção...

6.1 Características do Modelo Implementado

O modelo de implementação simplificado não inclui algumas características previstas no protocolo aqui apresentado, conforme listado a seguir:

- A agência de publicidade não foi introduzida como participante do protocolo; assim, a mediação entre empresa e sítio anunciante é feita diretamente pelo sistema, que mantém um cadastro tanto de empresas quanto dos sítios anunciantes e controla todas as interações entre eles;
- No modelo implementado, a responsabilidade de criação dos cupons é do próprio sistema, que centraliza todo o processo; no protocolo proposto a criação dos cupons

é feita pela empresa;

- A implementação não fez uso da Protocoladora Digital de Documentos Eletrônicos e por isso, não há “carimbos de tempo” em nenhuma das etapas;

- A questão da auditoria dos arquivos de log, tanto na empresa quanto no sítio anunciante, também não foi implementada;

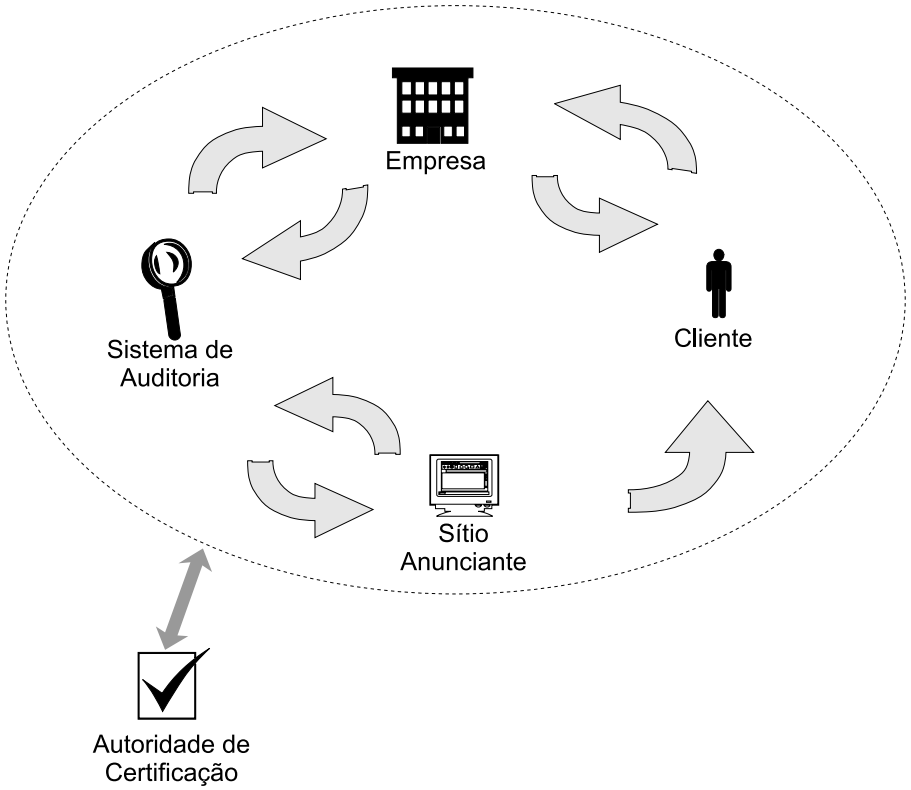


Figura 6.1: Esquema simplificado do protocolo implementado. Na implementação, o Sistema de Auditoria passa a controlar todo o processo mais ativamente: ele cadastra empresas e sítios anunciantes, cria os cupons, controla a distribuição e também o resgate destes. Não há agência de publicidade nem PDDE como participantes.

A figura 6.1 ilustra de forma simplificada o modelo implementado. O Sistema de Auditoria, caracterizado por um software voltado à Web, tem as seguintes atribuições:

- Cadastrar empresas e sítios anunciantes que participarão de esquemas de distribuição de cupons eletrônicos;

- Criar cupons eletrônicos que são assinados simultaneamente com as chaves públicas da empresa e do sítio;

- Participar da distribuição dos cupons feitas pelo sítio anunciante, mantendo uma base de dados com estas informações;

- Participar do resgate do cupom, validando-o no momento em que a empresa recebe o cupom do cliente;

6.1.1 Funcionamento do Modelo Implementado

Em seu Trabalho de Conclusão de Curso, Karl e Pasa descrevem as interações do sistema como a seguir [KAR 02]:

1. Uma empresa, cadastrada previamente no sistema, cadastra uma campanha de marketing, passando como informação dados como a arte gráfica da campanha, vantagens que o cliente obtém, público-alvo, quantidade de cupons, data de início e expiração da campanha. Assim que a campanha for criada, a empresa recebe uma especificação para que inclua um pequeno trecho de código em sua página que fará a procura pelo cupom. Logo, a campanha ficará aberta para pesquisas no sistema para sítios anunciantes que se cadastrarem;

2. Ao pesquisar e encontrar uma campanha que seja compatível com o tipo de público que possui, um sítio anunciante solicita a permissão à empresa para veicular a sua campanha. Se a empresa negar a permissão, a interação não prossegue, até que o sítio anunciante consiga encontrar alguma empresa que aceite a veiculação da campanha em seu sítio;

3. Quando receber a permissão para a veiculação, o sítio anunciante recebe também as informações de como veicular em seu sítio o cupom em forma de um “banner”

convencional, apenas tendo um conteúdo e tratamento interno diferentes dentro do sistema;

4. Um cliente ao ver a exibição do banner e realizar o clique sobre o mesmo, acionoará o sitema que se encarregará de passar o cupom ao cliente. O cliente poderá verificar a qualquer momento os cupons que possui guardados acessando o sistema e requisitando tais dados;

5. No processo de resgate do cupom, o programa incluído previamente na página da empresa testa se o cupom do cliente é válido consultando o sistema que, além de validar o cupom, poderá informar qual sítio anunciante passou o cupom ao cliente.

6.1.2 Aspectos de Segurança

Com relação aos aspectos de segurança do modelo implementado, Karl e Pasa fazem as seguintes considerações [KAR 02]:

- Os cupons são assinados digitalmente com a chave pública da empresa e a privada do sistema, assim quando um cupom chegar nas mãos da empresa, esta mesma pode obter os dados de volta (utilizando a chave pública do sistema e mais a sua privada);

- O tráfego entre o cliente e o servidor de serviços é feito através de conexão segura utilizando SSL (Security Socket Layer);

- Os dados sobre os cupons são armazenados na forma binária e cifrada no sistema, de modo a protegê-los contra possíveis ataques;

A Figura 6.2 mostra o modelo inicial da base de dados criado para a proposta de implementação:

6.2 Tecnologias Adotadas

As tecnologias escolhidas para a implementação estão listadas a seguir:

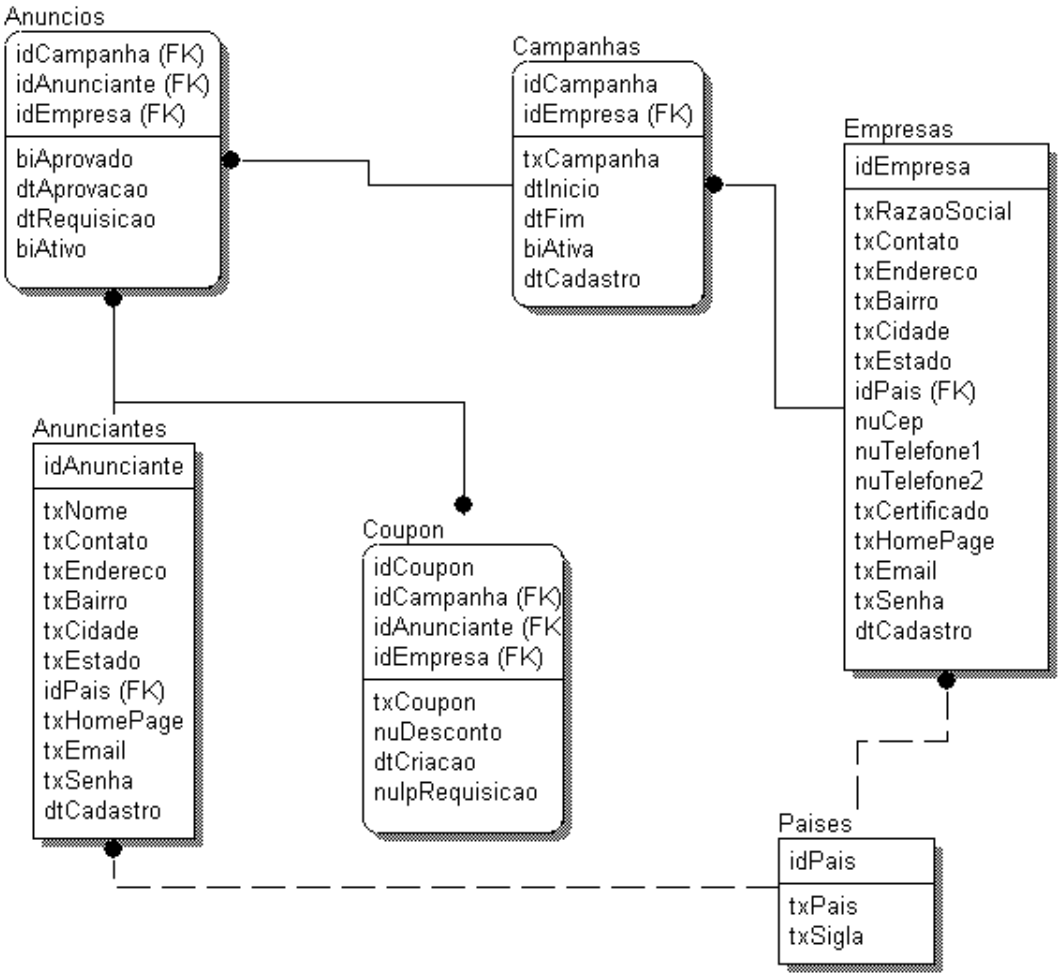


Figura 6.2: Modelo da Base de Dados do Sistema Implementado A figura mostra as classes envolvidas no sistema com seus atributos e os relacionamentos entre elas.

- **SSL:** A segurança no tráfego das informações entre os participantes é garantida por uma conexão que utiliza SSL (Secure Socket Layer);
- **PHP:** O PHP, uma linguagem de *script* com código aberto, foi a linguagem escolhida para o desenvolvimento do software;
- **XML:** O formato XML foi escolhido como padrão para a transmissão de informações entre os participantes;
- **MySQL:** Todos os dados gerados pelo sistema serão armazenados numa base de dados MySQL;

- **Linux/Apache:** O sistema operacional escolhido para o servidor foi o Linux e o servidor Web;

6.3 Formato de Apresentação

A figura 6.3 mostra a tela principal do sistema, montado para funcionar integralmente através da Web com a utilização de um navegador.

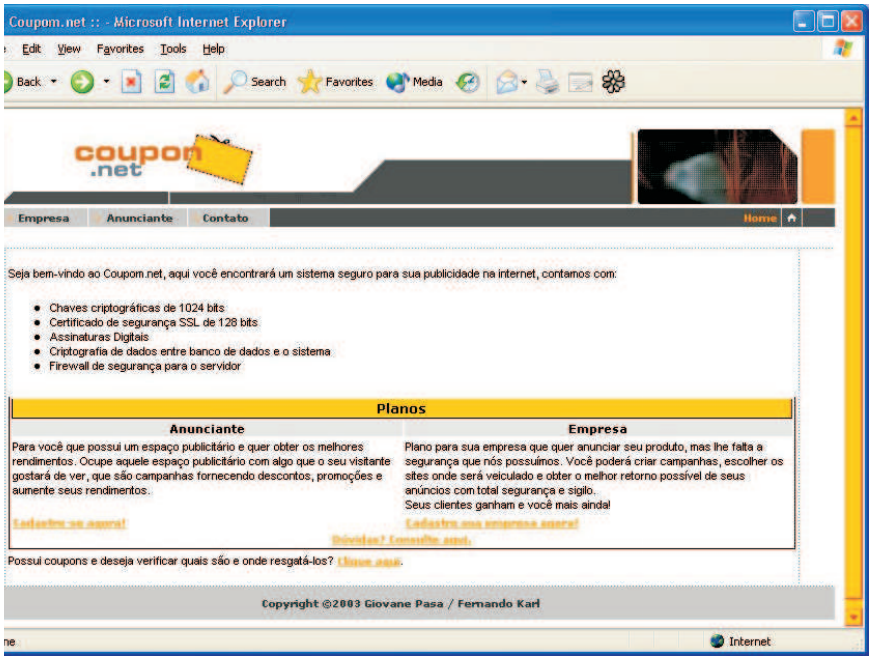


Figura 6.3: Tela principal de acesso ao sistema. A tela principal de acesso ao sistema possui links que permitem o acesso dos participantes através de sua autenticação (*login*) para obter informações sobre o sistema de publicidade.

A figura 6.4 mostra a tela de interação do sistema com a empresa, onde ela pode consultar todas as informações referentes às campanhas publicitárias que criou acompanhando a evolução de distribuição e resgate de cupons.

A figura 6.5 mostra tela de interação do sistema com o sítio anunciante, onde este pode acompanhar o processo de distribuição e resgate de cupons.

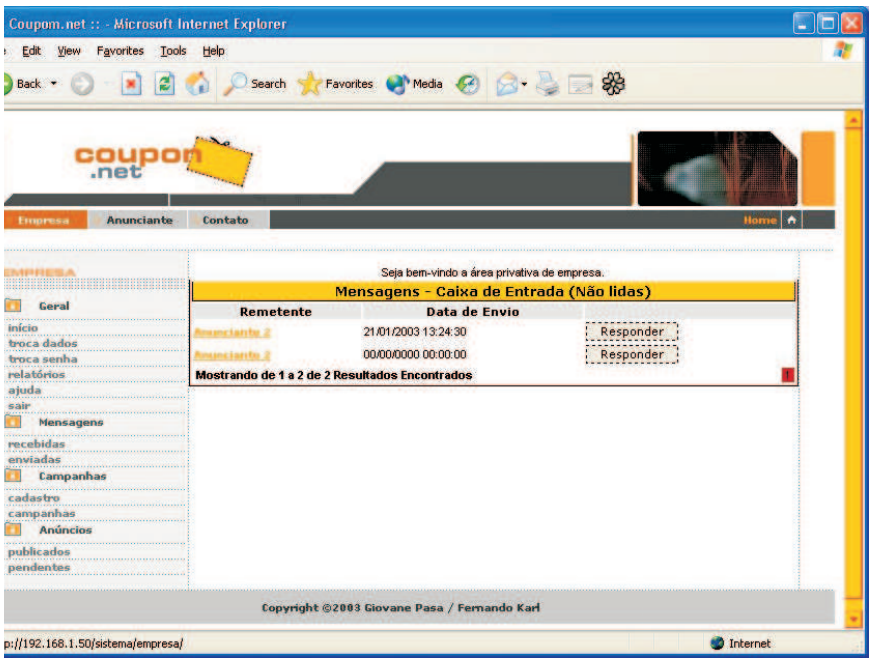


Figura 6.4: Tela de interação da empresa com o sistema. A empresa pode acessar todas as informações referentes a campanhas publicitárias que criou.

6.4 Conclusão

Este capítulo descreveu o modelo simplificado do protocolo implementado por alunos de graduação da Universidade Federal de Santa Catarina.

Por tratar-se de uma simplificação, esta implementação não atende a todos os requisitos previstos na descrição do protocolo. A seguir, tais requisitos estão listados a descrição de como são tratados na implementação:

1. **Efetividade para a empresa:** A medição da efetividade dos anúncios é garantida através dos cupons eletrônicos resgatados pelos clientes, tal como está previsto no protocolo.

2. **Efetividade para a agência de publicidade:** Este requisito não é atendido pela implementação já que este participante não existe;

3. **Efetividade para o sítio anunciante:** O **sítio anunciante** recebe as informações

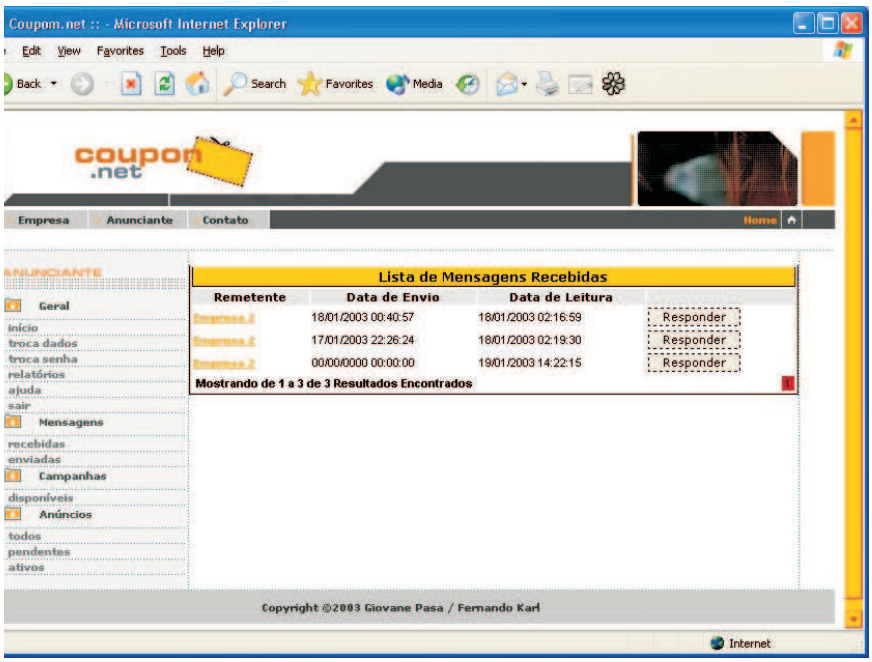


Figura 6.5: Tela de interação do sítio anunciante com o sistema. O sítio anunciante também pode acessar todas as informações referentes a campanhas publicitárias nas quais esteja envolvido.

do **Sistema de Auditoria** e pode constatar quantos dos cupons emitidos por ele chegaram até a **empresa**;

4. **Vantagem para o cliente:** Os cupons eletrônicos trazem as vantagens para o **cliente** em forma de promoções ou descontos durante aquisição de bens ou serviços da **empresa**;

5. **Auditoria do contrato de publicidade:** Este requisito não é atendido pela implementação diretamente; porém, como o sistema possui controle total da distribuição dos cupons aos clientes, ele pode fornecer informações relevantes para a **empresa**, auxiliando na estimativa de auditoria do contrato de publicidade;

6. **Medição da audiência:** Do mesmo modo como descrito no item anterior, os mecanismos para medir a audiência podem ser feitos apenas com base em estimativas a partir da distribuição de cupons pelo **sítio anunciante**;

7. **Privacidade para o cliente:** Os dados pessoais do **cliente** são preservados durante a execução de todas as etapas do protocolo implementado;

8. **Proteção dos participantes:** A intervenção direta do **Sistema de Auditoria** desde a criação do cupom até o seu resgate, garante que nenhum dos participantes envolvidos poderá fraudar o protocolo.

Como é possível observar, maior parte dos requisitos propostos são atendidos completa ou parcialmente pelo modelo implementado.

Finalmente, a descrição detalhada deste projeto pode ser encontrada em [KAR 02].

Capítulo 7

Análise e Especificação

7.1 Introdução

Neste capítulo serão apresentadas a modelagem, a especificação e a análise do protocolo proposto.

Conforme afirmam os autores coreanos Gang-Soo Lee e Jin-Seok Lee em [LEE 97] “a especificação formal e a análise de protocolos, bem como uma rigorosa prova matemática da segurança dos algoritmos criptográficos, são muito importantes”.

A modelagem do protocolo será apresentada através de Redes de Petri com o auxílio de duas ferramentas (HPSim e ARP) que serão descritas no decorrer do capítulo.

Assim sendo, a seção 7.2 apresentará uma breve introdução à semântica das Redes de Petri. Em seguida, a seção 7.3 apresentará o modelo graficamente. Após isso, a especificação e a análise serão descritas na seção 7.4 e, finalmente, a conclusão do capítulo será apresentada na seção 7.5.

7.2 As Redes de Petri

Segundo Cardoso em [CAR 97], uma Rede de Petri é um modelo formal para modelagem de sistemas que pode se apresentar de forma gráfica, matricial ou por um

conjunto de regras. Aqui será utilizada basicamente a forma gráfica que oferece vantagem sobre outras ferramentas de mesma natureza porque permite “obter informações sobre o comportamento do sistema modelado, através da análise de suas propriedades, gerais ou estruturais”.

Os grafos de Redes de Petri possuem basicamente quatro elementos:

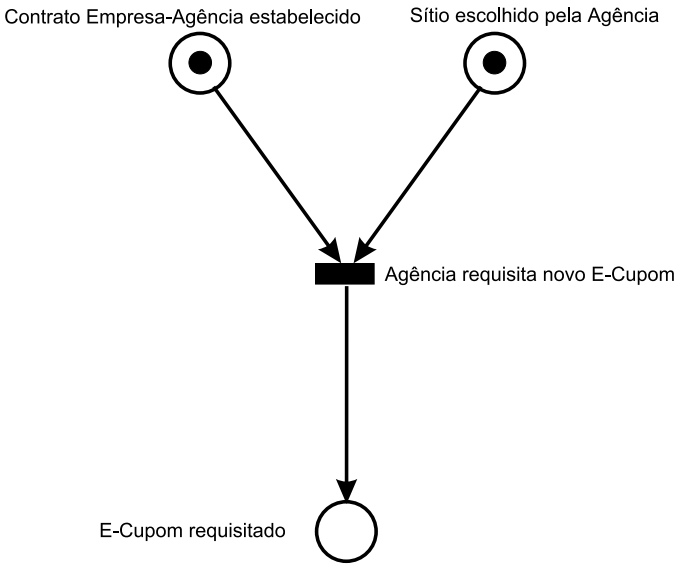
1. ***Lugar:*** é representado por um círculo e pode ser interpretado como uma condição, um estado parcial, uma espera, etc. Um *lugar* pode conter zero ou mais *fichas*.

2. ***Transição:*** é representada por uma barra ou um pequeno retângulo e está associada a um evento que ocorre no sistema. Uma *transição* está apta a ser executada quando houver *fichas* em todos os *lugares* que a precedem. Neste caso, as *fichas* são automaticamente transportadas para os *lugares* que a sucedem.

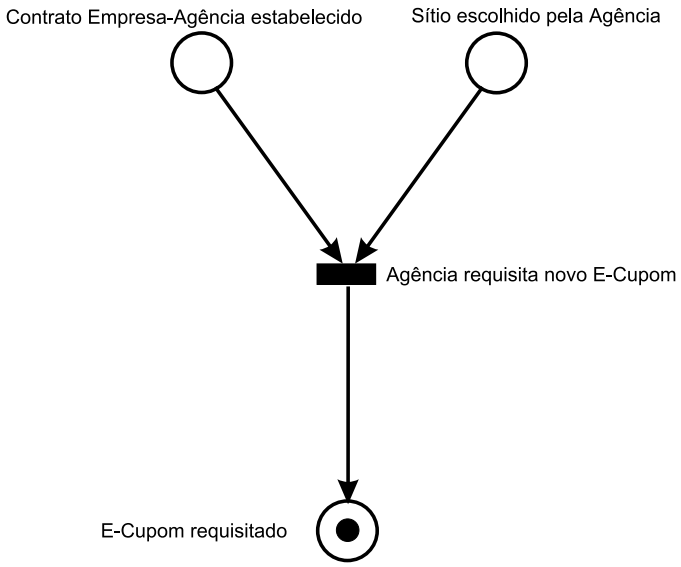
3. ***Ficha:*** é representada por um ponto (pequeno círculo) dentro de um *lugar*. Quando há uma *ficha* em um *lugar* (ponto dentro de um círculo) significa que a condição ou estado representado pelo *lugar* é verdadeira ou está satisfeita naquele momento.

4. **Arco:** é representado por um linha com uma seta que indica a direção em que o sistema é executado, ou seja, o movimento das *fichas* de um *lugar* para outro através de uma *transição*.

Um exemplo de Redes de Petri está representado na figura 7.1. Neste exemplo, há duas representações da mesma rede em dois diferentes estados. O estado **(a)** possui *fichas* em ambos os *lugares* que aparecem na parte superior. Isto indica que ambas as pré-condições são verdadeiras, ou seja, neste momento ali representado o contrato Empresa-Agência já foi estabelecido e o Sítio já foi escolhido pela Agência. Conforme já foi descrito, **quando todas as pré-condições são verdadeiras a *transição* está apta a ser executada**. Em outras palavras, considerando a semântica do exemplo, a requisição de um novo E-Cupom pela Agência só poderá ocorrer depois que o contrato Empresa-Agência estiver estabelecido e também depois que o Sítio Anunciante já tiver sido escolhido. Assim, a *transição* “Agência requisita novo E-Cupom” é executada de modo que as



a) Estado Inicial



b) Estado Seguinte após a Execução

Figura 7.1: Exemplo de uma Rede de Petri representada graficamente. Este exemplo mostra uma pequena rede em dois estados possíveis: o estado inicial (a) onde há uma *ficha* em cada um dos dois *lugares* superiores indicando que ambas as condições são verdadeiras; e o estado posterior à execução (b) onde a *transição* ocorre pois e as *fichas* são transportadas para o terceiro *lugar* da rede, na parte inferior.

fichas são transportadas para o *lugar* “Novo E-Cupom requisitado”, ou seja, esta última condição é que passa a ser verdadeira. Isto é o que está representado no estado seguinte **(b)** que aparece nesta figura de exemplo.

Vale salientar que existem inúmeros outros conceitos relacionados a Redes de Petri, além de diversas outras formas de uso e interpretação. Nesta seção foram descritos apenas os conceitos mais elementares para permitir o mínimo entendimento do modelo que será apresentado. Maiores detalhes sobre Redes de Petri podem ser encontrados em [CAR 97] e numa diversidade de outras bibliografias relacionadas com o tema.

7.3 A Modelagem do Protocolo Através de Redes de Petri

O protocolo apresentado neste trabalho foi **modelado** com o uso de Redes de Petri onde foi possível também fazer a **simulação** do funcionamento do protocolo. Para isto, foi usado o software HPSim versão 1.1, criado por Henryk Anschuetz e que, segundo especificações contidas no software, ele pode ser usado livremente para fins acadêmicos e de pesquisa. O programa foi obtido através da internet no endereço http://home.t-online.de/home/henryk.a/petrinet/e/hpsim_e.htm em janeiro de 2002.

7.3.1 Modelo Geral do Protocolo

Um modelo do protocolo proposto é apresentado na figura 7.2. Ele apresenta todas as etapas do protocolo quando ele é executado normalmente.

Seguem alguns comentários sobre o modelo apresentado:

- O modelo apresenta o sistema em seu estado inicial, isto é, com a **marcação inicial** das *fichas* nos três *lugares* que aparecem no topo da rede. Além disso, foram previamente colocadas fichas em três outros *lugares* da rede para garantir que, quando a rede for executada (simulação), as *transições* que dependem destas condições possam ser disparadas.

- Há duas *transições* no modelo cuja representação gráfica difere das demais pois os retângulos não estão preenchidos. Elas aparecem no canto inferior esquerdo da rede

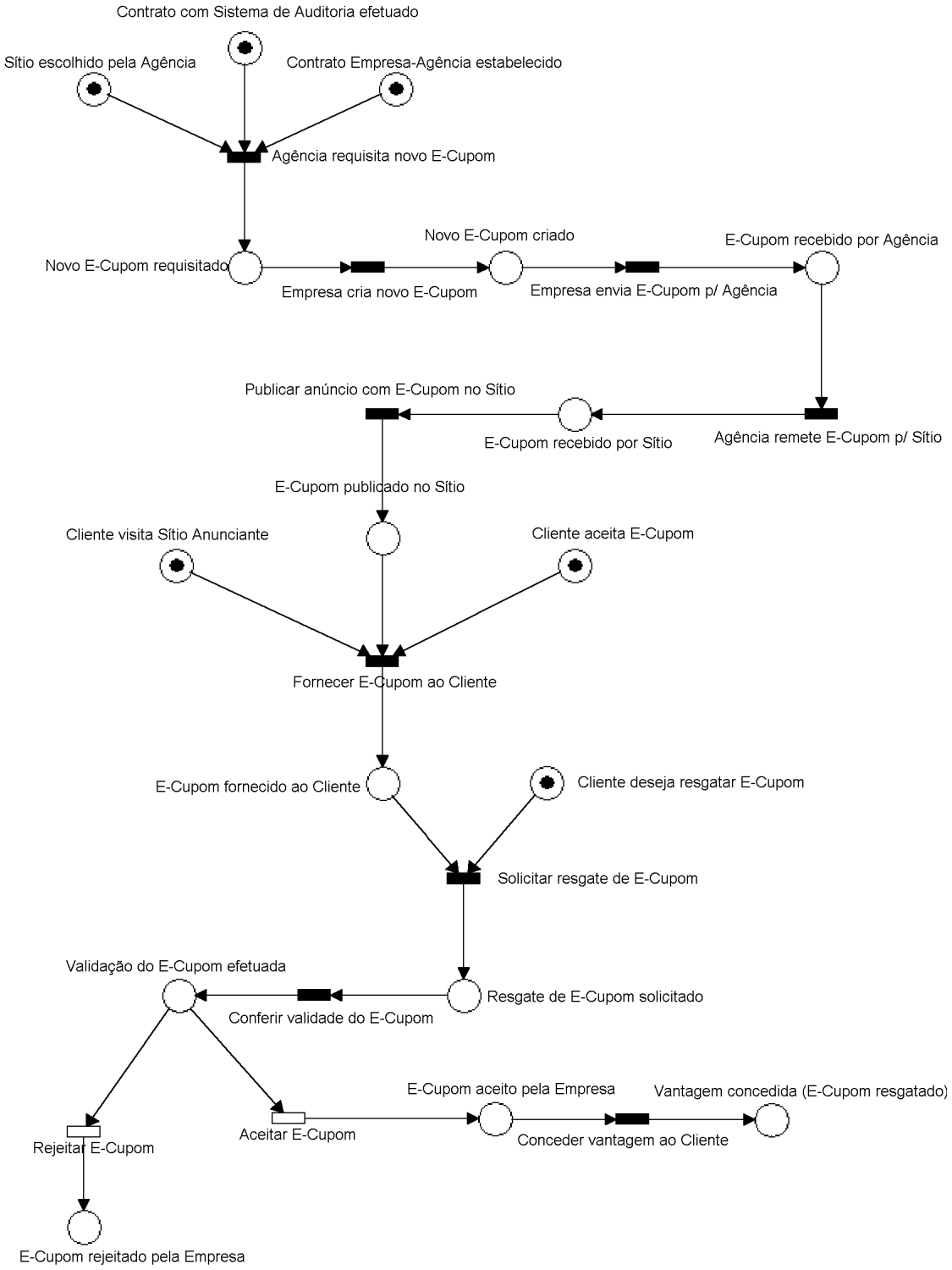


Figura 7.2: Modelo do protocolo proposto através de Redes de Petri. Este modelo apresenta as etapas do protocolo proposto.

e estão assim desenhadas porque são ***transições* temporizadas**, ou seja, um tempo aleatório de disparo foi aplicado a cada uma delas de modo que, quando o *lugar* que as precede estiver marcado com *ficha*, **apenas uma delas será disparada**. Esta característica foi adicionada ao modelo para simular as duas possibilidades que podem ocorrer após o recebimento do E-Cupom pela Empresa: ela pode aceitá-lo ou, dependendo de certas condições já declaradas, rejeitá-lo.

7.4 A Análise do Protocolo Através de Redes de Petri

A análise do protocolo através de Redes de Petri foi feita com o uso do software ARP versão 2.4, criado no Laboratório de Controle e Microinformática (LCMI), na Universidade Federal de Santa Catarina (UFSC), durante o trabalho de mestrado do Prof. Dr. Carlos Maziero. O software possui licença GPL (GNU General Public License) que permite o uso, a cópia e a distribuição livres. O programa foi obtido através da Internet no endereço http://www.ppgia.pucpr.br/ maziero/diversos/petri/arp.html em janeiro de 2002.

O software permite a especificação, simulação e análise de diversas características de uma Rede de Petri. As possibilidades alcançadas pelo software estão descritas no manual [Lab 89] disponível na mesma página da Internet acima citada.

7.4.1 A Especificação da Rede com ARP

Conforme descrito no manual do software ([Lab 89]), a linguagem de descrição de redes de Petri usada no ARP possui uma sintaxe semelhante à do Pascal, permitindo a identificação de lugares e transições por nomes quaisquer com até 20 caracteres. A estrutura básica de um texto de descrição de rede é a seguinte:

```
NET nome_da_rede;
   CONST
      {declaracao de constantes}
   NODES
      {declaracao dos nodos (lugares e transicoes)}
   STRUCTURE
      {declaracao da estrutura (arcos)}
ENDNET.
```

A declaração CONST permite descrever todas as constantes que se deseja utilizar na rede, tal como acontece na linguagem Pascal.

A declaração NODES é dividida em duas partes: a declaração de transições (*transition*) e a de lugares (*place*).

A declaração STRUCTURE permite descrever os arcos que ligam as transições aos lugares, sendo que, para cada transição, deve ser escrita a seguinte linha:

```
transicao: (lugares de entrada) , (lugares de saida);
```

Com esta linguagem bastante simples, a rede pode ser totalmente especificada. Maiores detalhes sobre a especificação podem ser encontrados no manual do software ARP ([Lab 89]).

A seguir é transcrita a especificação da Rede de Petri que representa o protocolo apresentado neste trabalho com o software ARP:

```
Net Auditoria_Web ;

Nodes

 { notacao: AP=Agencia de Publicidade,
            EM=Empresa,
            SA=Sitio Anunciante,
            CL=Cliente,
            SA=Sistema de Auditoria }

 AP_requisita_cupom, EM_cria_cupom,
 EM_envia_cupom, AP_envia_cupom,
 SA_publica_anuncio, SA_fornece_cupom,
 CL_solicita_resgate,
 EM_valida_cupom, EM_concede_vantagem        : Transition;
 EM_aceita_cupom, EM_rejeita_cupom           : Transition [0,5];

 SA_escolhido, AU_contratado, AP_contratada,
 SA_visitado, Cupom_aceito,
 Resgate_desejado                            : Place(1);

 Cupom_requisitado, Cupom_criado,
 AP_recebe_cupom, SA_recebe_cupom,
 Cupom_publicado, Cupom_fornecido,
 Resgate_solicitado, Validacao_efetuada,
 Vantagem_concedida,
 Cupom_rejeitado, Cupom_validado             : Place;


Structure

 AP_requisita_cupom      : (SA_escolhido, AU_contratado, AP_contratada),
                           (Cupom_requisitado);
 EM_cria_cupom           : (Cupom_requisitado), (Cupom_criado);
 EM_envia_cupom          : (Cupom_criado)     , (AP_recebe_cupom);
 AP_envia_cupom          : (AP_recebe_cupom)  , (SA_recebe_cupom);
```

```
 SA_publica_anuncio      : (SA_recebe_cupom)   , (Cupom_publicado);
 SA_fornece_cupom        : (Cupom_publicado, SA_visitado, Cupom_aceito),
                           (Cupom_fornecido);
 CL_solicita_resgate     : (Cupom_fornecido, Resgate_desejado),
                           (Resgate_solicitado);
 EM_valida_cupom         : (Resgate_solicitado), (Validacao_efetuada);
 EM_rejeita_cupom        : (Validacao_efetuada), (Cupom_rejeitado);
 EM_aceita_cupom         : (Validacao_efetuada), (Cupom_validado);
 EM_concede_vantagem     : (Cupom_validado)    , (Vantagem_concedida);
endNet.
```

7.4.2 Análise da Enumeração de Estados

A análise que será apresentada aqui trata-se da Enumeração de Estados e baseia-se na busca de todos os estados alcançáveis pela rede através do disparo de suas transições. Segundo o manual do software ARP [Lab 89], as propriedades analisadas são as seguintes:

- **Limitação:** é calculado o número máximo de fichas (limite) em cada lugar da rede, para os estados alcançáveis. Os lugares podem ser nulos, quando nunca receberam fichas; binários, sempre possuindo uma ou nenhuma ficha; limitados, quando o número de fichas é sempre igual ou inferior a um limite finito maior que 1 ou não-limitados, quando o número de fichas tende ao infinito (simbolizado por w).

- **Conservação:** é verificado se a soma total de fichas na rede é constante para qualquer marcação alcançável, indicando se a rede é estritamente conservativa ou não.

- **Vivacidade:** este teste é relativo ao disparo das transições. Uma transição é viva se, a partir de qualquer estado do grafo gerado, existe uma seqüência de disparos que a contenha, ou seja, que leve a seu disparo. Uma transição é quase-viva se foi disparada ao menos uma vez durante a construção do grafo.

- **Multi-sensibilização:** a enumeração de classes de estados em redes com temporização pode levar a resultados incorretos caso alguma transição esteja multi-sensibilizada no grafo. Uma transição está multi-sensibilizada se, para alguma marcação, o número de fichas na entrada da transição é maior ou igual a duas vezes o peso da entrada, para todos os lugares de entrada.

- **Reiniciação:** a rede é reiniciável se todos os seus estados forem reiniciáveis. Um estado é reiniciável se, partindo dele, existe alguma seqüência de disparos de transições que leve de volta ao estado inicial.

- ***Livelocks:*** é um ciclo de disparos de transições do qual a rede não possui saída, repetindo sempre os mesmos estados sem possibilidade de mudança de rumo. Caso sejam detectados live-locks na rede, são indicados os estados que iniciam cada um dos mesmos.

- ***Deadlocks:*** um estado em *deadlock* está bloqueado, não possuindo nenhuma transição sensibilizada e portanto nenhum estado sucessor. Caso sejam detectados deadlocks na rede, são indicadas as seqüências de disparos de transições que levam aos mesmos.

A seguir segue a transcrição do resultado apresentado pelo software na análise de Enumeração de Estados e cuja avaliação encontra-se na tabela 7.1

```
State Enumeration : net Auditoria_Web (12 reachable states).

Verified properties:
*--------------------------------------------------------------------------*
Net under analysis is binary.
  Null places (M = 0): {}
  Binary places      : {all}
  k-Bounded places   : {}
  Unbounded places   : {}

Net under analysis is not strictly conservative.

Multi-enabled Tr.: {}

Net under analysis is not live.
  Live Tr.         : {}
  "Almost-live" Tr.: {all}
  Non-fired Tr.    : {}

Net never can go back to M0.

No live-locks detected.

States (and fire sequencies) in deadlock:
  C10  :AP_requisita_cupom EM_cria_cupom EM_envia_cupom AP_envia_cupom
        SA_publica_anuncio SA_fornece_cupom CL_solicita_resgate
        EM_valida_cupom EM_aceita_cupom EM_concede_vantagem
  C11  :AP_requisita_cupom EM_cria_cupom EM_envia_cupom AP_envia_cupom
        SA_publica_anuncio SA_fornece_cupom CL_solicita_resgate
        EM_valida_cupom EM_rejeita_cupom
*--------------------------------------------------------------------------*
```

Tabela 7.1: Principais características do protocolo modelado: Conforme os resultados apontados pelo programa utilizado para a análise da rede, pode-se destacar as características abaixo:

Característica Avaliada	**Observação**
Limitação	Binária, pois os lugares representam apenas valores booleanos
Conservação	A rede não é estritamente conservativa pois a soma total de fichas na rede não é constante para qualquer marcação alcançável
Vivacidade	Todas as transições são quase-vivas pois são disparadas ao menos uma vez durante a execução da rede
Reiniciação	Não, pois analisando o grafo da rede pode-se observar que as marcações iniciais **Sítio Anunciante escolhido**, **Sistema de Auditoria contratado** e **Agência de Publicidade contratada** não recebem nenhuma entrada de outro caminho pois o objetivo da rede é modelar a criação de apenas um E-Cupom
LiveLock	Não foi detectado nenhum *livelock*
DeadLock	As transições **Empresa rejeita cupom** e **Empresa valida cupom** apresentam avisos da possibilidade de *deadlock*; entretanto, como ambas as transições estão temporizadas, supõe-se que apenas uma delas será executada de cada vez

7.5 Conclusão

A ferramenta HPSim foi utilizada para modelar e simular graficamente o protocolo. A especificação e análise da Enumeração de Estados foi feita com o software ARP. Em ambos os casos, durante o processo de modelagem e especificação, o protocolo foi alterado e melhorado pois as ferramentas permitiram encontrar alguns pontos que necessitavam de ajustes nas versões preliminares.

Esta situação comprovou, na prática, que a formalização auxilia no entendimento, garante a padronização e aponta falhas que geralmente não são encontradas numa especificação informal.

Capítulo 8

Considerações Finais

O presente trabalho apresentou um protocolo criptográfico para um sistema de publicidade na Web. Entende-se aqui por "sistema de publicidade" o conjunto de transações envolvidas num contrato de publicação de anúncios na Internet. Dentre as possíveis formas de publicidade, este trabalho trata mais especialmente da exposição de anúncios em forma de *banners* e de necessidades de medição relacionadas a estes anúncios.

Os estudos feitos acerca da publicidade convencional demonstraram que existem inúmeros métodos de medição de audiência utilizados atualmente. Os institutos Ibope, Marplan e IVC são os mais conhecidos no que diz respeito a este tipo de aferição em vários veículos de comunicação. As técnicas utilizadas para medir audiência variam de acordo com o veículo de comunicação escolhido.

Além disso, para diversos veículos de comunicação, é possível averiguar também se os anúncios estão sendo publicados exatamente da forma como foi previamente combinado entre as partes envolvidas. Em muitos casos, quando o veículo de comunicação não cumpre com as diretrizes previstas em contrato[1], podem ser estabelecidas formas de compensação (reapresentação do anúncio gratuitamente, por exemplo) ou até mesmo certas punições como multas contratuais.

[1] Algumas destas diretrizes podem ser, por exemplo, o tamanho do anúncio numa mídia impressa ou a fidelidade das cores, do texto, enfim, a qualidade de apresentação; no caso de TV e rádio, elas dizem respeito ao tempo de exposição, horário, número de ‘´inserções" do anúncio, entre outras características.

Conforme foi apresentado neste documento, o mesmo tipo de aferição aplicado aos anúncios expostos na Internet não constitui-se numa tarefa trivial. As características peculiares deste meio de comunicação acabam por dificultar a medição precisa tanto no que diz respeito à efetividade dos anúncios (quantos deles reverteram-se em vendas) quanto à verificação de que um anúncio esteja sendo publicado da forma como foi previamente contratado.

Este trabalho teve como objetivo apresentar uma proposta para solucionar ambos os problemas de medição em um sistema de publicidade na Internet. Para isso, foi construído um modelo de protocolo criptográfico baseado na proposta de cupons eletrônicos. A partir desta idéia, foram implementados novos elementos com o objetivo de adicionar outras funcionalidades e aumentar o nível de confiabilidade dos resultados obtidos na proposta de cupons eletrônicos.

Entre as inovações apresentadas neste protocolo, uma delas é a inclusão de um novo participante, a **agência de publicidade**, responsável por intermediar o contrato de publicidade entre a **empresa** e o **sítio anunciante**.

A implementação de um **Sistema de Auditoria** constitui-se em outra novidade desta proposta. Os objetivos são: averiguar se os anúncios estão sendo publicados conforme acordado previamente, medir a audiência do sítio anunciante e controlar o resgate de cupons junto à empresa.

O uso de uma **Protocoladora Digital de Documentos Eletrônicos**, que tem a responsabilidade de autenticar eletronicamente os documentos que transitam no sistema (cupons eletrônicos), adicionando a eles um “carimbo de tempo” confiável é outro importante diferencial desta protocolo.

A análise do protocolo foi feita através de Redes de Petri, comumente utilizadas para este fim.

Além disso, o projeto que implementou um protótipo deste protocolo, desenvolvido em paralelo com a dissertação, como trabalho de conclusão do curso de Ciência da Computação por aluno de graduação foi aqui apresentado.

Uma proposta para trabalho futuro seria a continuação do desenvolvimento do protótipo já implementado de forma a incorporar todas as características do

sistema. A formalização do protocolo através da linguagem ASN.1 também resultaria numa consolidação deste trabalho.

Finalmente, é importante salientar que este trabalho não pretende esgotar o tema, principalmente por reconhecer as dificuldades inerentes a aferição quando se trata de anúncios na Internet. Muitos trabalhos podem ser desenvolvidos a partir da proposta aqui apresentada, seja para aperfeiçoá-la ou para resolver outros problemas relacionados ao mesmo assunto e não contemplados neste trabalho.

Referências Bibliográficas

[ADA 01] ADAMS, C. et al. Internet x.509 public key infrastructure time stamp protocol (TSP). Internet Engineering Task Force, Agosto, 2001. Relatório técnico.

[BLU 02] BLUNDO, C.; CIMATO, S.; BONIS, A. D. A lightweight protocol for the generation and distribution of secure e-coupons. In: PROCEEDINGS OF THE ELEVENTH INTERNATIONAL CONFERENCE ON WORLD WIDE WEB, 2002. **Proceedings...** Honolulu, Hawaii, USA: ACM Press, 2002. p.542–552.

[BUR 01] BUREAU, I. A. **AAAA and IAB Interactive Marketing Unit (IMU) Study**. Publicado na WEB em março de 2001.

[CAR 97] CARDOSO, J.; VALETTE, R. **Redes de Petri**. Florianópolis: Editora da UFSC, 1997.

[CIM 01] CIMATO, S.; BONIS, A. D. Online advertising: Secure e-coupons. In: 7TH ITALIAN CONFERENCE ON THEORETICAL COMPUTER SCIENCE, 2001. **Proceedings...** Torino, Italy: Springer-Verlag, 2001. v.2202, p.370–383.

[CUS 01] CUSTÓDIO, R. F. Análise crítica da ICP-brasil: Resposta à consulta pública. Florianópolis: UFSC - Universidade Federal de Santa Catarina, Novembro, 2001. Relatório técnico.

[DIF 76] DIFFIE, W.; HELLMAN, M. E. New directions in cryptography. **IEEE Transactions on Information Theory**, [S.l.], v.IT-22, n.6, p.644–654, 1976.

[dMI 00] DE MÍDIA INTERATIVA, I. D. Método de auditoria eletrônica. IVC - Instituto Verificador de Circulação, Dezembro, 2000. Regimento InternoVersão 1.0.

[DOB 96] DOBBERTIN, H.; BOSSELAERS, A.; PRENEEL, B. RIPEMD-160: A strengthened version of RIPEMD. **Lecture Notes in Computer Science**, Berlim, v.1039, p.71–82, 1996.

[dPD 01] DE PESQUISA DATAFOLHA, I. **Credibilidade Da Mídia**.

[dPdIeA 00] DE POLÍTICA DE INFORMÁTICA E AUTOMAÇÃO, S. S. Evolução da internet no brasil e no mundo. Ministério da Ciência e Tecnologia (Brasil), Abril, 2000. Relatório técnico.

[ELG 85] ELGAMAL, T. A public key cryptosystem and a signature scheme based on discrete logarithms. **IEEE Transactions on Information Theory**, [S.l.], v.4, p.469–472, 1985.

[FER 99] FERREIRA, A. B. D. H. **Novo Aurélio Século XXI: O Dicionário Da Língua Portuguesa**. Rio de Janeiro: Editora Nova Fronteira, 1999.

[GAR 01] GARG, R. et al. An architecture for secure generation and verification of electronic coupons. In: USENIX ANNUAL TECHNICAL CONFERENCE, 2001. **Proceedings...** Boston, Massachussetts, EUA: [s.n.], 2001.

[GRI 99] GRITZALIS, S.; SPINELLIS, D.; GEORGIADIS, P. Security protocols over open networds and distributed systems: Formal methods for their analysis, design and verification. **Computer Communications - ELSEVIER**, [S.l.], v.22, p.697–709, 1999.

[HOU 02] HOUSLEY, R. et al. Internet x.509 public key infrastructure certificate and certificate revocation list (CRL) profile. Internet Engineering Task Force, Abril, 2002. RFC - Request for Comment3280.

[IBO 01] IBOPE. **Pesquisa Internet Pop**. Publicado na WEB em junho de 2001, no endereço: http://www.ibope.com.br/digital/produtos/internetpop.

[IGN 02] IGNACZAK, L. **Um Novo Modelo de Infra-Estrutura de Chaves Públicas Para Uso No Brasil Utilizando Aplicativos Com O Código Fonte Aberto**. Florianópolis: Universidade Federal de Santa Catarina, 2002. Dissertação de Mestrado.

[JAK 99] JAKOBSSON, M.; MACKENZIE, P. D.; STERN, J. P. Secure and lightweight advertising on the web. **Computer Networks**, [S.l.], v.31, p.1101–1109, 1999.

[JÚN 00] JÚNIOR, S. T. **Como Medir a Audiência Na Web**. Disponível em <http://www.centroatl.pr/edigest/edicoes2000/ed_set/ed7liet-tecnologia.html>. Acesso em: 10/09/2000.

[KAR 02] KARL, F. J.; PASA, G. Implementação de um sistema seguro de auditoria de publicidade na web. Florianópolis: Universidade Federal de Santa Catarina, Agosto, 2002. Trabalho de conclusão de curso.

[KOH 78] KOHNFELDER, L. M. **Towards a Practical Public-Key Cryptosystem**. Massachusetts Institute of Technology, 1978. Dissertação de Mestrado.

[Lab 89] Laboratório de Controle e Microinformática (LCMI) da Universidade Federal de Santa Catarina (USFC), Florianópolis. **Manual Do ARP: Analisador/Simulador de Redes de Petri**, dezembro, 1989.

[LAI 90] LAI, X.; MASSEY, J. L. A proposal for a new block encryption standard. In: ADVANCES IN CRYPTOLOGY - EUROCRYPT'90 PROCEEDINGS, 1990. **Proceedings...** Berlim: Springer-Verlag, 1990. p.389–404.

[LAI 91] LAI, X.; MASSEY, J. L. Markov ciphers and differential cryptanalisis. **EUROCRYPT 91 Proceedings**, [S.l.], v.547, p.17–38, 1991.

[LEE 97] LEE, G.-S.; LEE, J.-S. Petri net based models for specification and analysis of cryptographic protocols. **Journal of Systems Software**, [S.l.], v.37, p.141–159, 1997.

[MAR 99] MARTINS, Z. **Propaganda É Isso Aí!** São Paulo: Editora Futura, 1999.

[MEN 93] MENEZES, A. J.; VANSTONSE, S. A. Elliptic curve cryptosystems and their implementation. **Journal of Cryptology**, [S.l.], v.6, p.209–224, 1993.

[MEN 96] MENEZES, A. J.; OORSHCOT, P. C.; VANSTONE, S. **Handbook of Applied Cryptography**. Boca Raton: CRC Press, 1996.

[Nat 94] National Institute of Standards and Technology - NIST. Digital signature standard (DSS). National Institute of Sandards and Technology, Maio, 1994. Padrão recomendado (fips pub 186).

[Nat 95] National Institute of Standards and Technology - NIST. Secure hash standard. National Institute of Sandards and Technology, Abril, 1995. Padrão recomendado (fips pub 180-1).

[NEC 91] NECHVATAL, J. Public-key cryptography. NIST, Abril, 1991. NIST Special Publication800-2.

[NEC 00] NECHVATAL, J. et al. Report on the development of the advanced encryption standard (AES). National Institute of Standards and Technology, Outubro, 2000. Relatório técnico.

[NEG 95] NEGROPONTE, N. **A Vida Digital**. Companhia das Letras, 1995.

[ONG 85] ONG, H.; SCHNORR, C. P.; SHAMIR, A. Efficient signature schemes based on polynomial equations. **Advances in Cryptology: Proceedings of CRYTO'84**, [S.l.], v.196, p.37–46, 1985.

[PAS 01] PASQUAL, E. S. **IDDE - Uma Infra-estrutura para a Datação de Documentos Eletrônicos**. Florianópolis: Universidade Federal de Santa Catarina, 2001. Dissertação de Mestrado.

[PRE 00] PREDEBON, J. E. A. **Propaganda: Profissionais Ensinam Como Se Faz**. São Paulo: Editora Atlas, 2000.

[RIV 78] RIVEST, R. L.; SHAMIR, A.; ADLEMAN, L. M. A method for obtaining digital signatures and public-key cryptosystems. **Communications of the ACM**, [S.l.], v.21, n.2, p.120–126, 1978.

[RIV 92a] RIVEST, R. L. The MD4 message-digest algorithm. Internet Engineering Task Force, Abril, 1992. Relatório técnico.

[RIV 92b] RIVEST, R. L. The MD5 message-digest algorithm. Internet Engineering Task Force, Abril, 1992. Relatório técnico.

[RIV 94] RIVEST, R. L. The RC5 encryption algorithm. In: SECOND INTERNATIONAL WORKSHOP ON FAST SOFTWARE ENCRYPTION PROCEEDINGS, 1994. **Proceedings...** Leuven: Springer-Verlag, 1994. p.86–96.

[SCH 93] SCHNEIER, B. Description of a new variable-length key, 64-bit block cipher (blowfish). In: WORKSHOP ON FAST SOFTWARE ENCRYPTION PROCEEDINGS, 1993. **Proceedings...** Cambridge: Springer-Verlag, 1993. p.191–204.

[SCH 96] SCHNEIER, B. **Applied Cryptography, Second Edition: Protocols, Algorithms, and Source Code in C.** New York: Jon Wiley and Sons, 1996.

[SDI 00] SOCIEDADE DA INFORMAÇÃO, O. P. T. T. **Sociedade Da Informação No Brasil: Livro Verde**. Brasília: Ministério da Ciência e Tecnologia, 2000.

[STA 99] STALLINGS, W. **Criptography and Network Security: Principles and Practice**. New Jersey: Prentice-Hall, 1999.

[STI 95] STINSON, D. R. **Cryptography: Theory and Practice**. CRC Press, 1995.