FACULDADE DE TECNOLOGIA DE SÃO PAULO

Felipe Toshio Hirata

Segurança na WEB

São Paulo

FACULDADE DE TECNOLOGIA DE SÃO PAULO

Felipe Toshio Hirata

Segurança na WEB

Monografia submetida como exigência
parcial para a obtenção do Grau de
Tecnólogo em Processamento de Dados

Orientador: Prof. Sérgio Luiz Banin

São Paulo
2011

Resumo

O primeiro grande ataque, na web, ocorreu poucos anos após sua criação, em 1988. A partir deste momento, ficou claro a importância da segurança na rede, que na época era constituída de apenas sessenta mil servidores.

Desde então, cada vez mais lidamos com o tráfego de informações de extrema importância como informações bancárias ou pessoais, exigindo assim maiores cuidados.

Em 2010, foram gastos 14,8 bilhões de reais no comércio virtual brasileiro, atingindo 1/3 de todas as vendas de varejo feitas no país. Mais de 90% dos internautas brasileiros estão cadastrados em pelo menos uma rede social.

Com o crescimento da internet, o rápido desenvolvimento de novas tecnologias, o comércio virtual e os relacionamentos pessoais por meio da rede aumenta a cada dia devido à sua comodidade. Mas não são só as aplicações que foram aprimoradas. Os ataques também sofreram evoluções ao longo dos anos e, com eles a necessidade de melhores defesas e maior conhecimento por parte dos usuários.

Em vista disso, nesse trabalho analisamos diversos tipos de ataques, tanto especializados, que visam falhas em programação, quanto automatizados, que podem ser desferidos por pessoas sem grandes conhecimentos técnicos, bem como sua utilização através dos anos. Além disso, estudamos alguns métodos de defesa para ambos os tipos de ataques.

Abstract

The first big attack, on the web, happened a few years after it's creation, in 1988. From that moment on, it was clear the importance of security on the Internet, which at the time was made of only sixty thousand servers.

Since then, more and more we deal with the traffic of extremely important information such as bank accounts, passwords or personal information, what creates the need for special care.

In 2010, 14.8 billions of reais were spent in Brazilian e-commerce, becoming 1/3 of all sales made in the country. More than 90% of Brazilian INTERNET users are registered in at least one social network.

With the growth of the INTERNET, the fast development of new technologies, e-commerce and personal relationships through the web increase by the day, due to it's convenience. However it's not just the applications that suffered improvement. The attacks also evolved through the years and, along with them, the need of better defenses and further knowledge from the users.

Therefore, in this paper we analyzed several kinds of attacks, both specialized, which target flaws in programming, and automatized, which can be performed by people without a great amount of technical knowledge, as well as their use throughout the years. Furthermore, we studied some defenses methods for the two kinds of attacks.

Lista de Tabelas

Sumário

1 Introdução

A internet ja tem por volta de sessenta anos e, nesse tempo tem crescido extremamente rápido, com o rítimo acelerado do desenvolvimento tecnológico. Inúmeras possibilidades foram criadas e popularizadas com essa evolução, como a compra e venda de produtos, as transações bancárias e a socialização por intermédio da rede.

NOVA YORK […] Gastos de consumidores com compras on-line alcançaram US$ 38 bilhões no primeiro trimestre[...](O Globo, 2011)

O internet banking brasileiro já é o segundo canal de serviços mais utilizado pelos clientes, atrás apenas dos caixas automáticos (31%), respondendo por 23% das operações bancárias efetuadas no Brasil, segundo dados da Febraban (Federação Brasileira de Bancos), informa reportagem de Felipe Vanini Bruning para a Folha. (Folha, 2011)

Devido à comodidade desses novos serviços, a tendência é um crescimento ainda maior e, com esse intenso tráfego de informações de grande importância e/ou sigilo, como informações pessoais e econômicas, fica evidente o aumento da necessidade de segurança on-line. Como prova temos a FIGURA 1 – Gráfico com o total de incidentes, relacionados à segurança na internet entre 1999 e 2011, Reportados ao CERT.br. Brasil, setembro de 2011, que demonstra o crescimento de ocorrências na internet ao longo dos anos.

São Paulo - As fraudes de R$ 900 milhões registradas entre os anos de 2009 e 2010, de acordo com a Federação Brasileira de Bancos (Febraban) estão criando um cenário onde é cada vez maior a preocupação do setor de transações on-line (internet banking), bem como das empresas fabricantes de softwares de segurança em criar soluções para atender a este mercado. (Diário Comércio Indústria e Serviços, 2011)

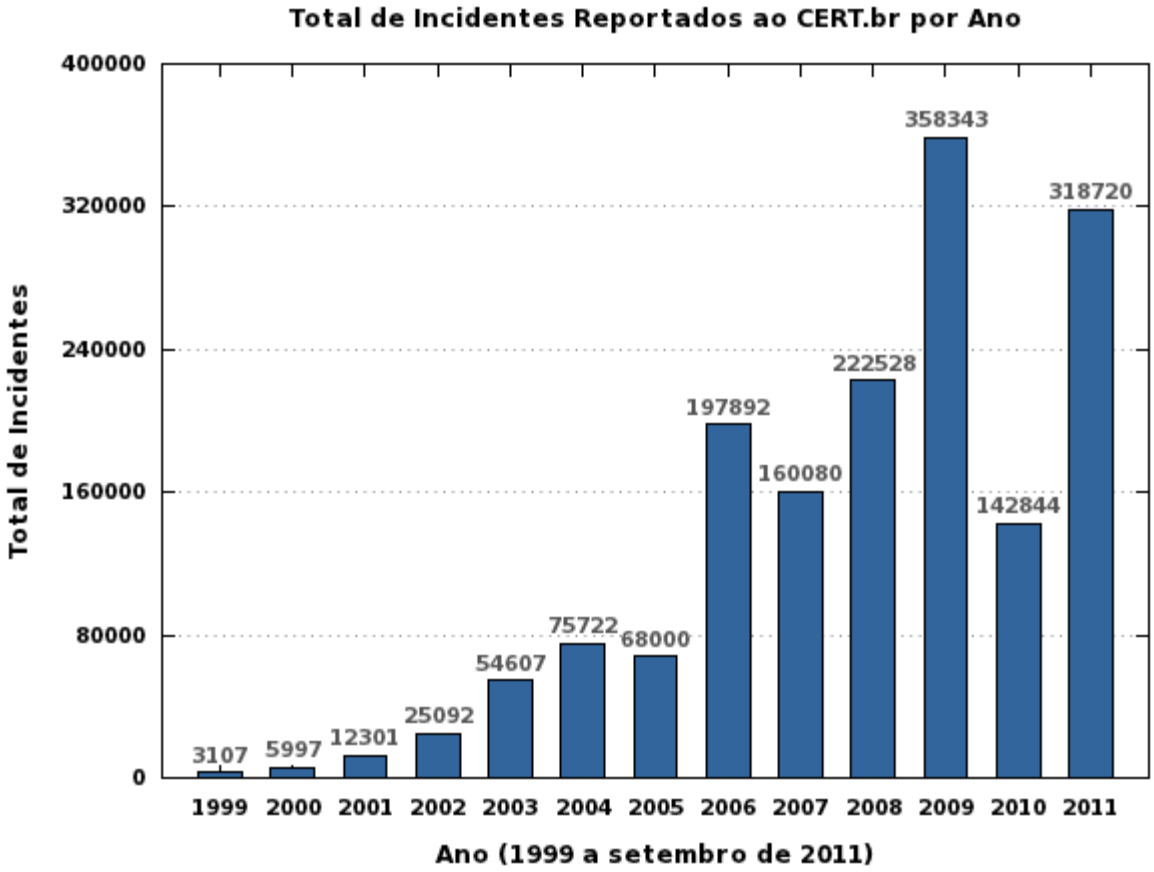

TABELA 1 – Gráfico com o total de incidentes, relacionados à segurança na internet entre 1999 e 2011, Reportados ao CERT.br. Brasil, setembro de 2011

Fonte: http://www.cert.br/stats/incidentes/

2 A Web

A internet é um conjunto de redes interligadas. Utilizando determinadas regras para a comunicação entre os computadores, conhecidos como protocolos de comunicação, as redes locais se ligam à redes de capacidades extremamente altas(Backbones), sustentados por agências governamentais ou corporações privadas, que por sua vez se conectam à outros backbones, criando assim uma rede mundial.

2.1 Serviços

A Web é formada por diversos tipos de serviços como o World Wide Web (WWW), o File Transfer Protocol(FTP), o correio eletrônico, o Internet Relay Chat (IRC) e o Telnet.

O World Wide Web (WWW) é a própria navegação em sites e utiliza o protocolo Hyper Text Transfer Protocol (htttp).

O File Transfer Protocol (FTP) é um protocolo que serve para a transferência de arquivos pela internet, de forma rápida e eficiente.

Utilizando os protocolos Post Office Protocol(POP) ou o Simple Mail Transfer Protocol(SMTP), o serviço correio eletrônico é responsável pela troca de dados entre computadores ou E-mail.

O Internet Relay Chat (IRC) é um serviço da internet que permite a troca de mensagens de texto, entre os usuários, em tempo real.

E, finalmente o Telnet é um serviço que permite o acesso à outros computadores na rede.

3 Ataques

O primeiro grande ataque ocorreu em 1988, quando um estudante da universidade de Cornell criou um worm, programa que se propaga através de vulnerabilidades ou falhas de configuração de software criando cópias de si mesmo. O ataque atingiu mais de 6000 computadores dos 60000 que constituíam a internet.

Este ataque levantou questões de segurança, que até o momento não eram consideradas já que a internet era um ambiente pequeno visto como amigável por seus desenvolvedores e usuários. 15 dias depois foi criada a CERT(Conputer Emergency Response Team), equipe que estuda vulnerabilidades de segurança na internet, pesquisa mudanças a longo-prazo em sistemas de rede e desenvolve informação e treinamento para auxiliar a melhorar a segurança.

Nos anos 90 surgiram o www, os browsers netscape e internet explorer e, com isso, as ferramentas de busca como o google e o yahoo, os spams, o hotmail (ferramenta de email na web), o comércio digital e os blogs. Em 97, a web já possuia mais de 1.000.000 de sites. Nessa década, são popularizados os cavalos de Tróia, sniffers e ataques de negação de serviços, alem da utilização da engenharia social.

Os cavalos de tróia são programas nocivos que se passam por programas úteis ou inofensivos como por exemplo arquivos recebidos por emails de conhecidos como fotos ou apresentações de slides. Algumas funções maliciosas são: a instalação de keyloggers, programas que capturam e armazenam as teclas digitadas pelos usuários; a alteração ou destruição de arquivos e a criação de backdoors possibilitando outros ataques.

Os sniffers são programas que capturam todo o tráfego de um segmento de rede e podem ser utilizados por administradores de rede, na segurança, ou por pessoas má-intencionadas, para a captura de senhas, por exemplo.

Os ataques de negação de serviços consistem no envio de pacotes de várias origens para um alvo, com o objetivo de desativar seus serviços temporariamente.

A engenharia social consiste em se passar por funcionários da empresa alvo ou autoridades interessadas em comprar ou prestar serviços para conseguir informações para o ataque, utilizando da falta de conhecimento dos usuários da rede.

Entre 2002 e 2004 são criadas as redes sociais facebook e orkut e o download de musicas pela rede é cada vez maior. No Brasil é criada a possibilidade de entrega da declaração do imposto de renda pela internet. Neste ponto existem mais de 20.000.000 de sites na web. Durante este período explode o número de códigos maliciosos como worms, bots, cavalos de tróia, vírus ou spywares.

Um bot é um programa capaz de se replicar automaticamente e de se comunicar com o invasor. Por meio dessa comunicação, um invasor pode executar um ataque de negação de serviços, adquirir informações do computador hospedeiro, enviar emails de phishing(envio de mensagem em que o remetente se passa por uma instituição conhecida como bancos ou empresas para a indução de instalação de softwares mal-intencionados ou conseguir informações sigilosas) ou spam.

Os vírus são programas ou partes de código, geralmente maliciosos que, ao serem executados, são ativados e inserem cópias de si mesmo em outros arquivos ou programas do computador.

Spyware é uma categoria de software que monitora as atividades de um sistema e as envia para terceiros.

As FIGURAS 2, 3 e 4, abaixo ilustram a distribuição dos tipos de ataques entre 2002 e 2004 e a predominância e crescimento dos ataques com vírus, bots e worms.

Descrição das categorias de incidentes demonstrados nas imagens:

-Worm: denominação utilizada para abranger notificações de atividades maliciosas relacionadas com o processo automatizado de propagação de códigos maliciosos na rede.

-DoS (Denial of Service): notificações de ataques de negação de serviço.

-Invasão: um ataque bem sucedido que resulte no acesso não autorizado a um computador ou rede.

-Web: um caso particular de ataque visando especificamente o comprometimento de servidores Web ou desfigurações de páginas na Internet.

-Scan: notificações de varreduras em redes de computadores, com o intuito de identificar quais computadores estão ativos e quais serviços estão sendo disponibilizados por eles. É amplamente utilizado por atacantes para identificar potenciais alvos, pois permite associar possíveis vulnerabilidades aos serviços habilitados em um computador.

-Fraude: Segundo Houaiss, é "qualquer ato ardiloso, enganoso, de má-fé, com intuito de lesar ou ludibriar outrem, ou de não cumprir determinado dever; logro". Esta categoria

engloba as notificações de tentativas de fraudes, ou seja, de incidentes em que ocorre uma tentativa de obter vantagem.

-Outros: notificações de incidentes que não se enquadram nas categorias anteriores.

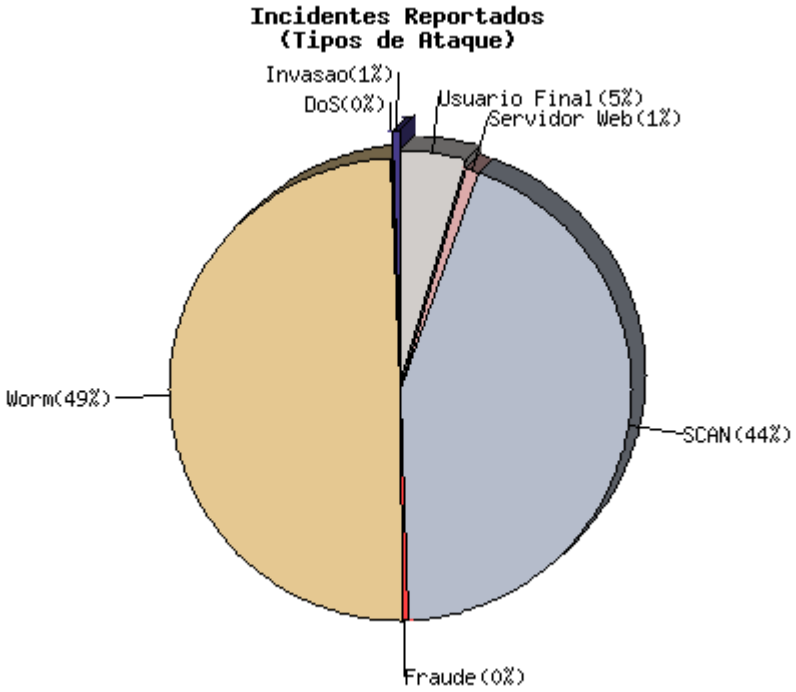

TABELA 2 – Gráfico mostrando a distribuição dos 25.092 incidentes, relacionados a segurança na internet, reportados ao CERT.br no ano de 2002. Brasil, dezembro de 2002
Fonte: http://www.cert.br/stats/incidentes/

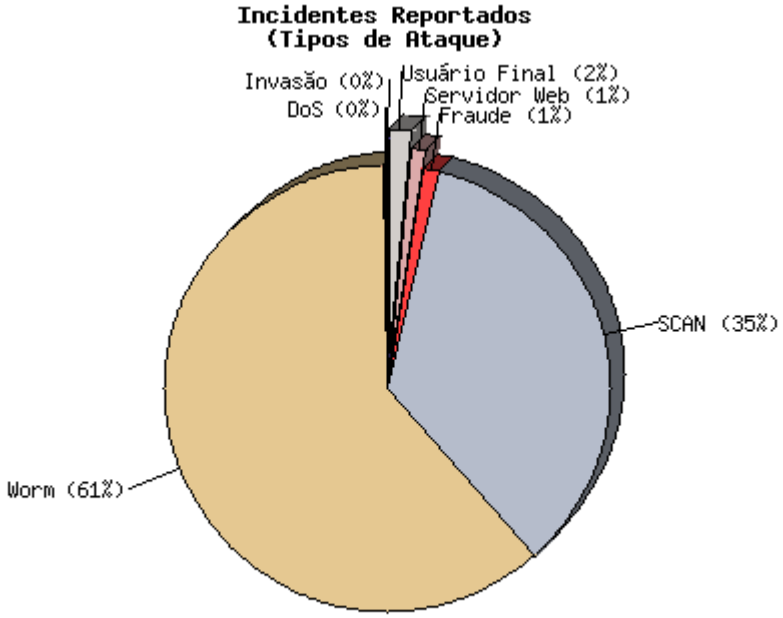

TABELA 3 – Gráfico mostrando a distribuição dos 54.607 incidentes, relacionados a segurança na internet, reportados ao CERT.br no ano de 2003. Brasil, dezembro de 2003
Fonte: http://www.cert.br/stats/incidentes/

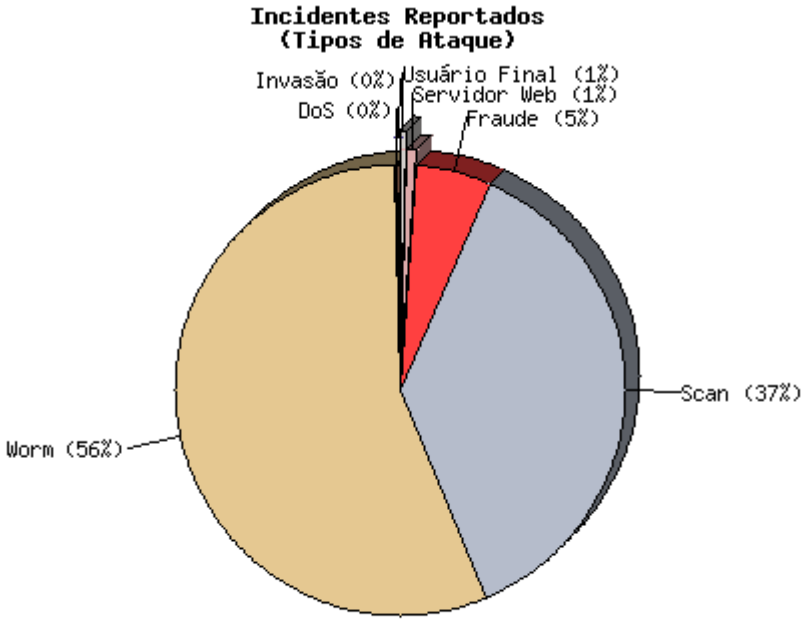

TABELA 4 – Gráfico mostrando a distribuição dos 75.722 incidentes, relacionados a segurança na internet, reportados ao CERT.br no ano de 2004. Brasil, dezembro de 2004
Fonte: http://www.cert.br/stats/incidentes/

De 2005 a 2009, a utilização das redes sociais tem aumentado exponencialmente. Em 2008, no Brasil, a receita federal recebeu 23,9 milhões de declarações de imposto de renda pela internet, de um total de 24,2 milhões.

A partir daí, o alvo dos ataques migra para os usuários finais. Devido a vasta quantidade de ferramentas prontas, os atacantes precisam cada vez menos de conhecimento especializado e é través de redes mal-configuradas, vulnerabilidade nos sistemas e da falta de conhecimento dos usuários que são realizados ataques com vírus, worms e bots visando obter informações dos usuários.

Nas imagens a seguir, podemos ver o crescimento das ocorrências de fraude. Cada vez mais os atacantes se utilizavam de phishing e engenharia social para obter os dados de usuários com pouca informação.

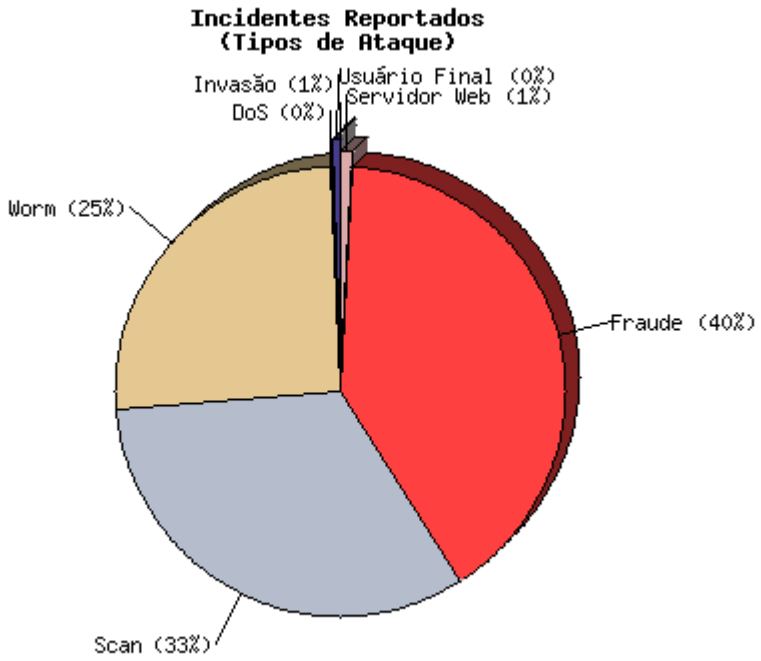

TABELA 5 – Gráfico mostrando a distribuição dos 68.000 incidentes, relacionados a segurança na internet, reportados ao CERT.br no ano de 2005. Brasil, dezembro de 2005
Fonte: http://www.cert.br/stats/incidentes/

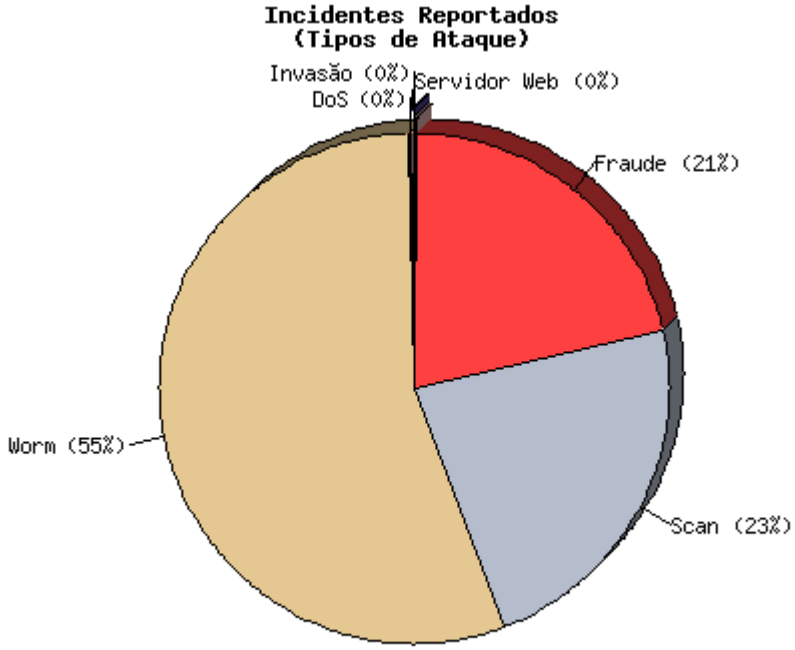

TABELA 6 – Gráfico mostrando a distribuição dos 197.892 incidentes, relacionados a segurança na internet, reportados ao CERT.br no ano de 2006. Brasil, dezembro de 2006
Fonte: http://www.cert.br/stats/incidentes/

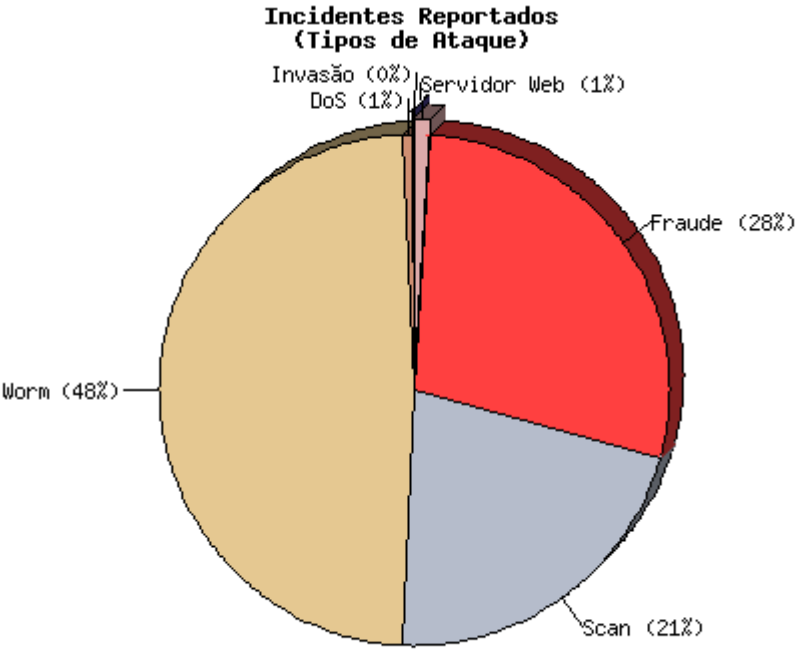

TABELA 7 – Gráfico mostrando a distribuição dos 160.080 incidentes, relacionados a segurança na internet, reportados ao CERT.br no ano de 2007. Brasil, dezembro de 2007
Fonte: http://www.cert.br/stats/incidentes/

TABELA 8 – Gráfico mostrando a distribuição dos 222.528 incidentes, relacionados a segurança na internet, reportados ao CERT.br no ano de 2008. Brasil, dezembro de 2008
Fonte: http://www.cert.br/stats/incidentes/

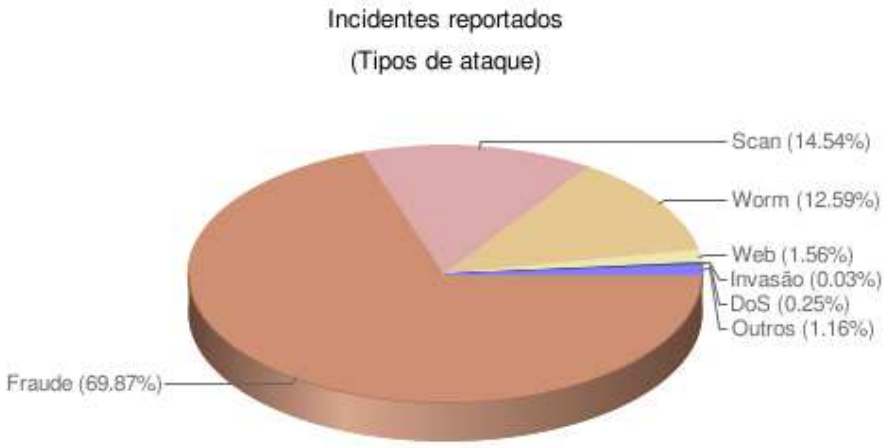

TABELA 9 – Gráfico mostrando a distribuição dos 358.343 incidentes, relacionados a segurança na internet, reportados ao CERT.br no ano de 2009. Brasil, dezembro de 2009
Fonte: http://www.cert.br/stats/incidentes/

A partir de 2010, devido à conscientização dos usuários sobre as possíveis ameaças na web através de reportagens e da publicação de informativos na própria rede, além da fortificação na segurança das aplicações web, as fraudes começaram a diminuir assim como ataques em geral, como mostram as FIGURAS 1, 10 e 11.

TABELA 10 – Gráfico mostrando a distribuição dos 142.844 incidentes, relacionados a segurança na internet, reportados ao CERT.br no ano de 2010. Brasil, dezembro de 2010
Fonte: http://www.cert.br/stats/incidentes/

TABELA 11 – Gráfico mostrando a distribuição dos 318.720 incidentes, relacionados a segurança na internet, reportados ao CERT.br no ano de 2011. Brasil, setembro de 2011
Fonte: http://www.cert.br/stats/incidentes/

4 Defesas

Para evitar ataques e amenizar as vulnerabilidades de um sistema, é aconselhável que os softwares utilizados estejam sempre atualizados, mas existem alguns meios de tornar a rede mais segura como o firewall, que evita o tráfego não-autorizado entre redes; a criptografia, que dificulta a leitura das informações enviadas e os antivírus, que previnem a ação de softwares mal-intencionados.

4.1 Firewall

Através do firewall, é possível filtrar quem acessa e que tipo de dados passam para a rede interna. Existem diversos tipos de firewall, dentre eles, os mais comuns são o filtro de pacotes, o Network Adress Translation (NAT) e o firewall de aplicação.

Os filtros de pacotes são aqueles que verificam os cabeçalhos dos pacotes e os comparam com as regras pré-definidas de controle de acesso, para então liberar ou não o fluxo de dados, controlando assim os dados destinados ao host.

O firewall Network Adress Translation (NAT) traduz os endereços de origem e destino, e controla as rotas dos pacotes que passam pelo host.

E, por fim, o firewall de aplicação, que age como um intermediário entre a rede interna e a externa, avaliando o número da seção TCP dos pacotes. Com isso é possível, até mesmo, verificar a relação de todo o tráfego de dados através firewall.

4.2 Criptografia

A criptografia são as técnicas utilizadas para fazer com que uma mensagem se torne legível apenas para quem a escreve e seu destinatário.

A criptografia se utiliza de códigos e cifras. enquanto os códigos substituem uma palavra ou frase por uma palavra, as cifras utilizam um algorítimo, fazendo com que a mensagem se torne somente um amontoado de letras.

Levando em conta os tipos de chave (valor ou algorítimo utilizados na codificação e decodificação dos dados), podemos classificar a criptografia em criptografia de chave privada ou pública. A criptografia de chave privada é aquela que utiliza a mesma chave para codificar e decodificar os dados; e a criptografia de chave pública utiliza chaves diferentes na codificação e decodificação dos dados.

A criptografia tem sido muito utilizada para a segurança de dados importantes na web como transações bancárias, por exemplo. Entre os métodos atuais, podemos destacar:

- Função de Hash Unidirecional: um algorítimo cuja codificação sempre resulta em um texto ininteligível e de tamanho fixo. Este método é muito utilizado na verificação da integridade de mensagens;
- Código de Autenticação de mensagem (MAC): como o próprio nome diz, este método é exclusivamente usado para a autenticação de uma mensagem. São mecanismos utilizados com uma chave secreta, que geram um código, com base na mensagem. Caso os dados sejam alterados por alguem que não possua a chave, o código gerado não corresponderia ao texto;
- Assinaturas Digitais: tipo de Código de Autenticação de mensagem, que utiliza uma chave pública e uma privada. Assim somente quem tem a chave privada poderia ter alterado os dados;
- Certificado Digital: é um documento eletrônico que contem a assinatura digital com os dados do utilizador, confirmando a identidade da pessoa ou entidade;

4.3 Antivírus

Os antivírus são programas que detectam e tratam de arquivos suspeitos. Esses programas se utilizam de várias técnicas para a detecção de vírus tais quais:

- O escaneamento de vírus conhecidos;
- A analise heurística, a qual consiste em verificar o código dos programas à procura

de instruções suspeitas;

- A verificação de integridade, onde é criado um banco de dados com informações sobre os arquivos do computador e sobre os setores do sistema, possibilitando emitir um alerta quando algo for alterado;

4.4 Programação

Existem ataques que se utilizam de falhas na programação. Neste trabalho, vou citar algumas e relacionar com as possíveis medidas de prevenção utilizando o Ruby on Rails.

O Ruby on Rails é uma linguagem relativamente nova, criada em 2003 por David Heinemeier hansson, que tem crescido muito em aplicações Web. Muitos sítios já estão utilizando a linguagem, entre elas o Twiter e o Scribd. A seguir, estão listados alguns ataques provenientes de erros na programação.

4.4.1 Roubo de Sessões e Replay

Sessões são o conjunto de dados a respeito do acesso de um usuário a uma aplicação. Esses dados tem por finalidade evitar a necessidade de constante identificação do usuário. As seções são formadas por um hash de valores e um id de seção. Esse id é armazenado em cada cookie recebido pelo usuário e a autenticação é feita com esses cookies, assim qualquer um que conseguir um cookie de outra pessoa pode acessar o sistema.

Para evitar que isso ocorra, o Ruby pode utilizar dois recursos. Um deles consiste em salvar o hash e o id de sessão do usuário em um banco de dados. Assim, nenhum dado é armazenado no computador do usuário. Apesar de resolver o problema de roubo de seção a performance do sistema cai. O segundo o hash é armazenado e encriptado no cookie do cliente, fazendo com que não haja necessidade de um id. Isso é feito com uma chave, preferencialmente aleatória, com menus de trinta caracteres, incluindo o código abaixo no arquivo enviroment.rb do Ruby.

Deve-se manter em mente que apesar de criptografados, nunca devemos deixar dados importantes em coockies. O Replay consiste em um indivíduo que conseguiu manter o coockiee utiliza-lo mais de uma vez, como por exemplo uma aplicação que mantem os dados sobre os créditos do usuário na sessão.

4.4.2 Fixação de sessão

Acontece quando o atacante cria uma sessão válida e, fazendo com que um cliente utilize o coockie criado por ele. Ao fazer a autenticação, o cliente faz com que o id do atacante se torne válida.

Uma solução para o problema seria fazer com que a autenticação transformasse qualquer id anterior em inválido. No Ruby conseguimos criar uma nova seção com o comando: *reset_session.*

Outra possibilidade seria salvar detalhes sobre o usuário na sessão, como a versão do navegador. Isso dificultaria a utilização do mesmo ID por mais de um usuário.

Uma alternativa seria definir um período de validade no cookie com o ID da seção. Para evitar que o usuário edite este período, as sessões teriam que ser expiradas no servidor. Além disso, o Ruby oferece a possibilidade de apagar sessões criadas a muito tempo, assim evitamos que o usuário utilize a mesma sessão várias vezes.

4.4.3 Upload de Arquivos

Existem aplicações que permitem o upload de arquivos e, às vezes o usuário pode fazer o upload de arquivos com nomes maliciosos, que poderiam sobrescrever arquivos importantes como por exemplo o nome ../../web/password. Este exemplo sobrescreveria o arquivo password. Uma solução possível seria não aceitar arquivos que possuam determinados caracteres em seu nome. Essa validação deve ser feita de forma assíncrona, pois uma validação de forma síncrona seria vulnerável a ataques de negação de serviço.

5 Conclusão

Considerando todas as informações reunidas, podemos constatar que sempre houveram ataques na web, desde sua criação, seja visando o roubo de informações ou simplesmente causar danos a outros usuários.

Graças à implementação e o desenvolvimento do comércio virtual, dos internet banks e de sites de Relações com Investidores, as informações que trafegam na rede ganharam uma importância tremenda, se tornando alvos de ataques.

E essa evolução ainda não parou. Certamente serão criados meios de conexão cada vez mais rápidos e cada vez mais dados serão digitalizados, aumentando assim a necessidade de métodos mais complexos de segurança.

Porém, como visto no trabalho, apesar dos estudos e desenvolvimento de novas técnicas de proteção de dados, os ataques na rede não pararam, mas sim se adaptaram às novas medidas.

Podemos concluir que independentemente do aperfeiçoamento dos métodos de defesa, sempre haverão pessoas buscando novos meios para evitá-las.

6. Referências Bibliográficas

ALECRIM, Emerson, **Entendendo a Certificação Digital** . Brasil, Info Wester, 2009. Disponível em <http://www.infowester.com/assincertdigital.php>. Acesso em: 02 abr. 2011.

ALMEIDA, Rubens Queiroz de, **A evolução da Internet** . Campinas, UNICAMP, 1998. Disponível em <http://www.ccuec.unicamp.br/revista/infotec/internet/internet1-1.html>. Acesso em: 23 out. 2011.

ARROYO, Alexandre; SANTOS, Fábio. Programação **para web utilizando PHP.** Campinas, UNICAMP, 2002.

CENTRO DE ESTUDOS, RESPOSTA E TRATAMENTO DE INCIDENTES DE SEGURANÇA NO BRASIL, **cartilha de segurança para internet**. Brasil, 2011. Disponível em <http://cartilha.cert.br/>. Acesso em: 14 nov. 2011.

CENTRO DE ESTUDOS, RESPOSTA E TRATAMENTO DE INCIDENTES DE SEGURANÇA NO BRASIL, **Estatísticas dos Incidentes Reportados ao CERT.br** . Brasil, 2011. Disponível em <http://www.cert.br/stats/incidentes/>. Acesso em: 23 out. 2011.

CENTRO DE ESTUDOS, RESPOSTA E TRATAMENTO DE INCIDENTES DE SEGURANÇA NO BRASIL, NÚCLEO DE INFORMAÇÃO E COORDENAÇÃO DO PONTP .BR E COMITÊ GESTOR DA INTERNET NO BRASIL, **Evolução dos problemas de segurança e formas de proteção**. Brasil, 2011. Disponível em <http://www.cert.br/docs/palestras/certbr-conbratec2005.pdf>. Acesso em: 14 nov. 2011.

DIÀRIO COMÈRCIO INDÙSTRIA E SERVIÇOS, **Internet já é o 2º maior canal bancário do país** . Brasil, 2011. Disponível em <Fraudes de R$ 900 mi estimulam bancos a investir em segurança>. Acesso em: 25 jun. 2011.

DISCOVERY, **A Internet** . Brasil, 2007. Disponível em

<http://discoverybrasil.uol.com.br/internet/interactivo.shtml?cc=BR>. Acesso em: 25 jun. 2011.

ÈPOCA, **Ciberterrorismo e Guerras Virtuais Preocupam Governos** . Brasil, 2009. Disponível em <http://revistaepoca.globo.com/Revista/Epoca/0,,EMI105832-15227,00.html>. Acesso em: 23 out. 2011.

FOLHA, **Internet já é o 2º maior canal bancário do país** . Brasil, 2011. Disponível em <http://www1.folha.uol.com.br/mercado/919401-internet-ja-e-o-2-maior-canal-bancario-do-pais.shtml>. Acesso em: 25 jun. 2011.

O GLOBO, **Gastos com compras via internet nos EUA sobem 12% no 1º trimestre** . Brasil, 2011. Disponível em <http://oglobo.globo.com/tecnologia/mat/2011/05/11/gastos-com-compras-via-internet-nos-eua-sobem-12-no-1-trimestre-924431684.asp>. Acesso em: 25 jun. 2011.

JASPER, Nichols Aron. **Historia, Técnicas e Classificação de Algoritmos Esteganográficos.** São Paulo, Fatec-SP, 2009. Disponível em <http://www.slideshare.net/NLDT/histria-tcnicas-e-classificao-de-algoritmo>. Acesso em: 02 abr. 2011.

KEHOE, Brendan P. **Zen and the Art of the Internet** . EUA, 1992. Disponível em <http://www.cs.indiana.edu/docproject/zen/zen-1.0_toc.html>. Acesso em: 23 out. 2011.

REBIT, **A Evolução da Internet – Anos 80** . São Paulo, 2010. Disponível em <http://rebit.com.br/2010/10/evolucao-da-internet-%E2%80%93-anos-80/>. Acesso em: 23 out. 2011.

REBIT, **A Evolução da Internet – Anos 90** . São Paulo, 2010. Disponível em <http://rebit.com.br/2010/10/evolucao-da-internet-%e2%80%93-anos-90/>. Acesso em: 23 out. 2011.

REBIT, **A Evolução da Internet – Últimos 10 anos** . São Paulo, 2010. Disponível em

<http://rebit.com.br/2010/10/evolucao-da-internet-ultimos-10-anos/>. Acesso em: 23 out. 2011.

RODRIGO**,** Luis. **Apostila do Curso de Segurança.** Petrópolis, Universidade Estácio de Sá, 2005.

TRINTA, Fernando Antonio Mota; MACÊDO, Rodrigo Cavalcanti de. **Um Estudo sobre Criptografia e Assinatura Digital**. Pernambuco, UFPE, 1998. Disponível em <http://www.di.ufpe.br/~flash/ais98/cripto/criptografia.htm>. Acesso em: 02 abr. 2011.

UOL, **Linha do Tempo: Internet** . Brasil, 2010. Disponível em <http://sobreuol.noticias.uol.com.br/historia/historia.jhtm>. Acesso em: 23 out. 2011.

VAZ, Paulo, **Cronologia da Internet** . Rio de Janeiro, UFRJ, 2001. Disponível em <http://www.febf.uerj.br/crono_web/cronologia_internet.html>. Acesso em: 23 out. 2011.

WEBER, Heiko. Ruby On Rails Security Guide EUA , 2008. Disponível em <http://guides.rubyonrails.org/security.html>. Acesso em: 02 abr. 2011.