Análise de Privacidade em Redes IP: Aspectos Técnicos e Jurídicos

Antonio Evangelista de Freitas, João Pedro Hallack Sansão e Victor Guimarães Ferreira

***Resumo*— A presente pesquisa é resultado de um estudo sobre segurança e privacidade na Internet. É realizada uma análise abordando a parte técnica da comunicação em redes IP apontando em quais camadas de rede pode-se obter informações que comprometam a privacidade do usuário ocasionando falha na segurança da rede. Algumas falhas de segurança de rede que comprometem a privacidade na rede foram exemplificadas. Como complementação dessa análise, obteve-se informações dos cabeçalhos dos pacotes de informação através de um *sniffer* de rede para que se possa inferir quais delas podem comprometer a privacidade dos usuários e como a legislação brasileira trata desse assunto. Também são analisados os principais aspectos jurídicos no Brasil que tratam sobre o limite e o alcance da segurança e privacidade do usuário na rede com enfoque na principal lei de regulação da Internet, o Marco Civil da Internet.**

Palavras-Chave*— *Privacidade na Internet. Segurança de rede. Marco Civil da Internet.

***Abstract*— This paper is the result of a study on security and privacy on the Internet. An analysis will be done by addressing the technical aspects of communication in IP networks pointing at which layers of the network is possible to obtain information that compromise user privacy causing failure in network security. Some network security breaches that compromise privacy on the network were exemplified. Given this study, we intend to get the header information via a network sniffer to be able to analyse which of them compromise the privacy of users and how the Brazilian legislation addresses this issue. The main legal issues in Brazil that deal over the limit and scope of security and user privacy in network will be discussed focusing on the main law regulating the Internet, the Marco Civil of Internet.**

Keywords: Privacy on the Internet. Network security. Marco Civil of Internet.

I. INTRODUÇÃO

A Internet hoje faz parte da vida de muitas pessoas, pois através dela podemos nos comunicar com todo o mundo. A Internet é utilizada direta ou indiretamente para fins de comunicação, compras, vendas, entretenimento e diversas outras aplicações. Diante do grande crescimento da Internet no mundo nos últimos anos, tornou-se necessário o desenvolvimento de técnicas de segurança mais robustas e bem elaboradas para que se consiga manter a privacidade dos usuários na rede. Informações pessoais estão cada vez mais difusas na Internet e isso está causando diversos tipos de crimes cibernéticos [1]. A presente pesquisa faz uma análise sobre o funcionamento e a importância da segurança em redes IP, apontando aspectos técnicos sobre como é possível obter informações que ferem a privacidade de usuários na rede e aspectos jurídicos que tratam sobre a regulação da Internet no Brasil.

II. PROTEÇÃO JURÍDICA À PRIVACIDADE

Após as denúncias de espionagem por parte dos EUA, o governo brasileiro passou a se dedicar à criação de políticas com relação à segurança e privacidade na Internet. Questões como falsificação de endereços, coleta ilegal de dados e filtragem de conexões devem ser previstas em lei para alcançar a punição dos responsáveis. Além disso, deve-se haver também uma certificação de equipamentos de telecomunicações atendendo a aspectos de segurança humana, física e lógica.

Diante da necessidade de regular o uso da Internet no Brasil, privilegiando a liberdade e segurança de acesso, o governo se apressou em aprovar o projeto de lei que já tramitava na Câmara desde 2011, o Marco Civil da Internet. Para o Marco Civil o acesso à Internet é essencial ao exercício da cidadania. O internauta tem garantia de que sua vida privada não será violada, a qualidade da conexão estará condizente com o contratado e que seus dados só serão repassados a terceiros se ele aceitar – ou em casos judiciais [2].

Os direitos e garantias dos usuários, expressos claramente no texto do Marco Civil, reforçam o direito a liberdade de expressão e a privacidade nas comunicações. O art. 7º do Marco Civil define que o acesso a Internet é essencial e assegura aos usuários seus direitos que têm como destaque a inviolabilidade do direito à privacidade na rede podendo esse ser motivo de indenização por dano material ou moral. É garantido o sigilo das comunicações, a manutenção da qualidade contratada e a não suspensão da conexão à internet, salvo por falta de pagamento.

III. ANÁLISE DA SEGURANÇA DO USUÁRIO

Para este trabalho utilizou-se um *sniffer* de rede (*WireShark*) para capturar pacotes de uma rede doméstica e analisá-los do ponto de vista da privacidade e da segurança da rede. Trata-se de uma ferramenta que utiliza *libcap* (biblioteca de captura de tráfego de rede) e tem como principal característica a possibilidade de remontar uma sessão. Além

disso, o *Wireshark* foi uma das primeiras ferramentas a tratar de pacotes específicos das redes sem fio.

Várias capturas foram realizadas em visitas a alguns *web sites*. Será feita uma análise dos campos dos cabeçalhos dos protocolos que podem conter informações relevantes para a segurança da rede. Um exemplo de tela de captura é exibido na Fig. 1.

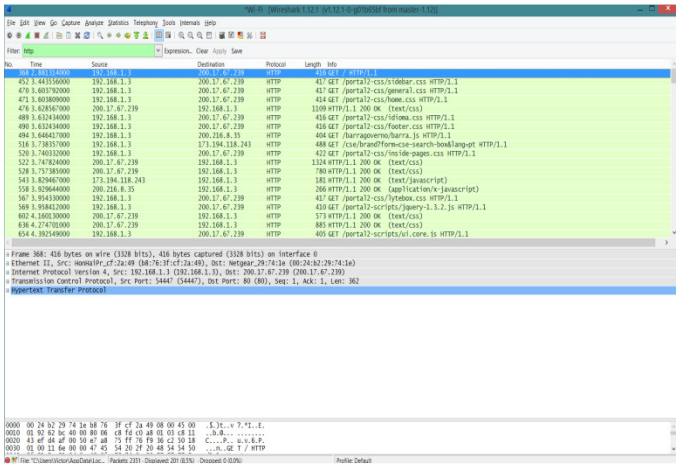

Fig. 1. Captura de tráfego

Com relação ao segmento TCP, podem-se destacar os campos "Sequence Number" e "Window Size". Existem ferramentas que, através dos valores desses campos, identificam o sistema operacional da máquina. Diante disso, um usuário malicioso pode explorar falhas de segurança específicas do sistema operacional identificado. Além desses campos, o valor "80" do campo Destination Port indica que o serviço utilizado é um servidor da Web (HTTP).

Os campos "Source" e "Destination" no cabeçalho IPv4 indicam os endereços IP de origem e destino da requisição. Por exemplo, o endereço de origem 192.168.1.3 se refere ao endereço IP do *notebook* utilizado (cliente) e o endereço de destino 200.17.67.239 se refere ao endereço do *site* da UFSJ (servidor) que foi acessado.

O endereço IP é o campo mais visado em ataques, pois identificando uma máquina, um usuário malicioso pode identificar um servidor para invadir ou pode ainda identificar individualmente um usuário, pois muitas das vezes uma máquina é utilizada apenas por uma pessoa. Além disso, endereços IP identificam também a rede de origem de um pacote e o fluxo de pacotes de uma conexão [3].

É possível identificar no *wireshark* também informações como login e senha que um usuário pode digitar para um *site*. Para isso é só procurar o método HTTP denominado POST. Este método é comumente utilizado para o envio de informações para o servidor requerido [1].

Para servir de exemplo, foi acessado o site da biblioteca da UFSJ, onde é requerido *login* e senha dos usuários para acessar o cadastro pelo qual é possível fazer busca, reserva e renovação de livros. Essas informações podem ser facilmente visualizadas na captura, pois o site da biblioteca da UFSJ não utiliza o protocolo SSL para criptografar os dados transmitidos entre o navegador e o servidor *web*.

Na pilha de protocolos TCP/IP não há controle e tratamento adequado sobre o tráfego de informações, sem uso de criptografia e controle de erro de bit na maioria das vezes. Estas falhas podem dar origem a uma série de ataques, dentre os quais os do tipo *Eavesdropping* (onde um atacante entra como mediador na comunicação entre dois pontos para capturar o tráfego que circula pela rede auxiliada pela configuração da placa de rede em modo promíscuo), como o IP *Spoffing* (com base em falhas de autenticação no protocolo IP da camada de rede), ARP *Spoofin*g (também baseado em falhas de autenticação no protocolo ARP na camada de enlace) e DNS*Spoofing* (baseado na alteração da tabela de endereçamento do protocolo DNS – *Domain Name System* - da camada de aplicação). Ou seja, um *Mac Adress* (endereço físico da placa de rede) colocado entre o usuário e o *Gateway* pode responder e receber por vários IP's diferentes. Desta forma, mesmo que um terceiro usuário atue como *Man-in-the-Middle* (intermediador) entre um determinado tráfego entre dois pontos de comunicação, haverá grande dificuldade para um usuário comum saber sobre a autenticidade e confiabilidade das informações que este estará recebendo, uma vez que o intermediador responde aos *requests* (requisições) como se fosse o *host* (hospedeiro) destino ou o usuário. Existe uma grande dificuldade em saber sobre a verdadeira identidade do agente coletor de informações e mesmo ainda sobre a existência deste. Além disso, o TCP/IP, não traz nenhum protocolo de controle para a camada física e de enlace, fato este que pode agravar ainda mais a questão da segurança e privacidade dos dados que ali circulam [4].

IV. CONCLUSÕES

Com o crescimento rápido da Internet no Brasil e no mundo, cresceu também o número de dados que circulam com informações privadas de usuários. Para que haja proteção mínima aos usuários na Internet tornou-se necessária a criação de legislação específica para regular a Internet a fim de obter um maior controle no uso da rede e que resguarde a privacidade dos usuários. As denúncias de espionagem por parte dos EUA ajudaram a acelerar o processo de aprovação da primeira lei específica que regula a Internet no Brasil, o Marco Civil da Internet. Tal lei se caracteriza como uma norma geral que se aplica a todos os elementos formadores da Internet e busca a proteção à privacidade do usuário.

Através de um processo de captura de pacotes em uma rede, pôde-se concluir que é possível reunir informações que seriam suficientes para um ataque cibernético e invasões na rede onde pode-se buscar dados pessoais, senhas, número de cartão de crédito e várias outras informações que caracterizam uma invasão à privacidade do usuário e uma falha na segurança da rede. Essa prática contraria expressamente o art. 7º inciso II do Marco Civil que garante a inviolabilidade e sigilo do fluxo de suas comunicações pela internet, salvo por ordem judicial, na forma da lei.

REFERÊNCIAS

[1] KUROSE, J. F., ROSS, K. W.. **Redes de Computadores e a Internet - Uma nova abordagem**. 5ª Edição. São Paulo: Addison Wesley, 2010.

[2] FERRAÇO, Ricardo. **Relatório final da CPI da Espionagem**. Abril de 2014.

[3] MELO, Marco Aurélio Vilaça de. **Aspectos Técnicos e Legais da Coleta e Anonimização de Tráfego de Redes IP**. 2009. 104f. Dissertação DCC - UFMG, Programa de Pós-Graduação em Ciência da Computação do Instituto de Ciências Exatas, BH – MG.

[4] TANENBAUM, Andrew S. **Redes de Computadores**. Tradução da 5ª ed. Rio de Janeiro: Campus Elsevier, 2011.