Universidade de São Paulo
Instituto de Ciências Matemáticas e de Computação

SCC0207 – Computadores e Sociedade

Espionagem de Atividade Computacional por meio de *Sniffers*

Elias Italiano Rodrigues – 7987251
Gabriel Dupim Hosino – 8066252
Lucas Nunes Arvani – 7986802
Rodolfo Megiato de Lima – 7987286
Rodrigo Rusa – 7986970

São Carlos, 20 de março de 2015

Sumário

1 Introdução

Este é um trabalho de pesquisa em que são apresentadas algumas informações a respeito de espionagem computacional por meio de *sniffers*, com a apresentação de leis e de um estudo de caso envolvendo o tema.

1.1 Espionagem de Atividade Computacional

O significado de espionagem consiste na prática de obter informações de caráter sigiloso relativas ao alvo sem sua prévia autorização. No caso, como se trata de espionagem de atividade computacional, esta é realizada sobre os dados armazenados em disco rígido ou sendo enviados ou recebidos através da rede.

A espionagem de atividade computacional é um termo fácil de ser definido, porém nem sempre é simples chegar a um consenso quando se trata de espionagem ou simplesmente de monitoramento. Seria espionagem apenas quando é feito um acesso externo à rede alvo? Poderia o monitoramento de um gerente de rede ser considerado espionagem?

1.2 *Sniffers*

Literalmente, *sniffer* significa "farejador", porém uma melhor tradução para o português seria "escuta"ou "grampo".

Sniffers podem ser implementados de duas maneiras: software ou hardware. Na primeira, um software é instalado diretamente no alvo ou em um outro sistema externo responsável por fazer o grampo. Já no caso de uma abordagem por hardware, um dispositivo físico é acoplado no meio onde a informação trafega. Em uma rede sem-fio, como os dados são transmitidos pelo ar, é mais simples capturar um pacote de dados, diferentemente de uma rede cabeada, onde o trafego é direcionado, normalmente é o cenário onde o uso do hardware de *sniffer* é feito. [1]

2 Como ocorre a espionagem?

Os motivos que levam a atividade de espionagem computacional são vários. Uns dos mais comuns são quando existe algum tipo de suspeita sobre ações de uma pessoa nos sistemas de TI de uma empresa ou instituição; espionagem para obter informações de vantagem competitiva; para testes de segurança; ou simplesmente por diversão/curiosidade.

3 Quais são as implicações?

3.1 Criptografia

Atualmente, com o advento do protocolo HTTPS, conhecido como o protocolo HTTP seguro, os ataques de *sniffing* são prevenidos, pois todas as informações das mensagens são criptografadas, dificultando muito a interpretação desses dados pelo atacante. Esse protocolo foi construído com o objetivo de prevenir esses tipos de ataques.

Assim, com o HTTPS, as mensagens não podem ser mais lidas por meio do ataque de *sniffing*, mas ainda é possível obter informações sobre remetente e o destinatário. Ainda assim, pode-se também realizar ataques *man-in-the-middle* e de *replay*, já que ainda há a captura do pacote.

Ataque *man-in-the-middle* é uma forma de ataque em que os dados trocados entre duas partes, por exemplo você e o seu banco, são de alguma forma interceptados, registrados e possivelmente alterados pelo atacante sem que as vítimas percebam. O atacante pode decidir retransmitir entre os legítimos participantes os dados inalterados, com alterações ou bloquear partes da informação. Já ataques de *replay* é uma outra forma de ataque onde o interceptador reproduz as mensagens interceptadas sem alterar o conteúdo.

3.2 Leis

Com relação as atividades de interceptações de comunicações de informática, no Brasil vigora a Lei Nº 9.296, de 24 de Julho de 1996 que segundo o artigo 10: "Constitui crime realizar interceptação de comunicações telefônicas, de informática ou telemática, ou quebrar segredo da Justiça, sem autorização judicial ou com objetivos não autorizados em lei." [2]

Nos Estados Unidos, também existe uma lei para privacidade de comunicações eletrônicas de 1986 que diz ser ilegal intencionalmente, ou propositadamente interceptar, divulgar ou usar o conteúdo de qualquer comunicação por fio, oral ou eletrônica através de o uso de um dispositivo de escuta. [3]

3.3 Caso

Segundo uma notícia publicada em 2011, o Google poderia ser investigado por interceptar, sem autorização judicial, dados privados de redes sem fio brasileiras. Segundo o pesquisador cearense Pablo Ximenes, professor de Ciência da Computação e pesquisador do Information Security Research Team (Insert), as interceptações aconteceram entre 2009 e 2010, durante o levantamento de dados para o Google Street View. [4]

Segundo Ximenes, as interceptações ilegais aconteceram por meio do sistema de coleta de dados de redes sem fio realizada pelo veículo autônomo da Google. Ele afirma que o veículo usou uma técnica de captura de dados conhecida como *sniffing*. Com ela, todas as ondas de rádio destinadas a uma rede sem fio eram interceptadas pela empresa. Isso inclui dados privados de usuários, como fotos, senhas, emails e documentos pessoais.

Em estudo realizado pelo Insert, foi constatado que o serviço da Google teria interceptado aproximadamente 4.300 redes sem fio apenas em Minas Gerais. Segundo Jairo Ponte, advogado e professor de Direito da Faculdade Cearense (FaC) a Google teria infrigido a lei federal 9.296/96, conhecida como Lei da Interceptação Telefônica, segundo o artigo 10.

Respondendo a acusação, a empresa admitiu que seu veículo interceptou redes sem fio, mas alegou só ter acessado redes públicas. Segundo a Google, os veículos capturaram apenas sinais do tipo *beacon*, mensagens públicas das redes sem fio. Em nova investigação, os pesquisadores desmentiram as declarações, ao provarem que a empresa também acessou *payloads*.

Para tentar resolver o impasse, o próprio Google encomendou uma análise de códigos e programas utilizados pelo Street View. O estudo confirmou as denúncias, provando que o

veículo coletou dados de conexões sem fio. Na lista apresentada pela análise, estavam emails completos, páginas web e senhas.

O Google justificou o fato, afirmando que as interceptações ocorreram de forma não-intencional. Segundo a empresa, tudo não passou de erro de programação dos engenheiros do Street View. Além disso, o Google alegou que apenas acessou informações incompletas, já que o veículo estava em movimento.

Pablo Ximenes afirma que as interceptações foram feitas de forma intencional. Um indício seria o registro da patente "aproximação de localização baseada em redes sem fio", proposta pelo Google em 2008 e registrada em janeiro de 2010. Entre outros, a patente descreve o mesmo mecanismo de captura de dados presente no veículo do Street View.

Para Ximenes, a ideia de que um erro no código de captura tenha passado despercebido é "no mínimo ingênua". "As rotinas de teste do Google estão entre as mais rigorosas do mundo. Se fosse um erro por parte dos engenheiros, duvido que ele não fosse sido resolvido ainda nos estágios de teste", ponderou o pesquisador.

Como consequência das pressões, o Google suspendeu a coleta de dados de redes sem fio nos carros do Street View. Essa medida continua em vigor até hoje. Apesar disso, ainda existe debate sobre quais foram as reais proporções das interceptações promovidas pelo serviço.

4 Conclusão

Os ataques envolvendo *sniffing* são inevitáveis, já que os pacotes trafegam livre nas redes sem-fio, portanto o uso de criptografia nos dados é essencial quando se trata de informações sensíveis. Mas mesmo com o conteúdo dos pacotes criptografados, as informações de cabeçalho são sempre disponíveis dando conhecimento sobre o tráfego realizado.

A realização de espionagem de atividades computacionais por meio de *sniffing* é considerada crime, se realizada sem ordem judicial, em vários países do mundo. Mesmo não sendo legal, a ocorrência desse tipo de ataque é bem frequente, por vários motivos já citados. Mas somente analisando cada caso de espionagem pode-se julgar se foi ético e moral ou não.

Referências

[1] James F. Kurose, Keith W. Ross. Computer Networking: A Top-down Approach. 6th Ed. pag.58-59,480.

[2] L9296
<http://www.planalto.gov.br/ccivil˙03/leis/l9296.htm>
Acesso em: 18 de março de 2015

[3] Wiretap Act - Lawyers.com
<http://communications-media.lawyers.com/privacy-law/wiretapping.html>
Acesso em: 18 de março de 2015

[4] Google: pesquisador cearense acusa o Street View de interceptação de dados - Lei e Ordem
<http://www.leieordem.com.br/google-pesquisador-cearense-acusa-o-street-view-de-interceptacao-de-dados.html>
Acesso em: 18 de março de 2015