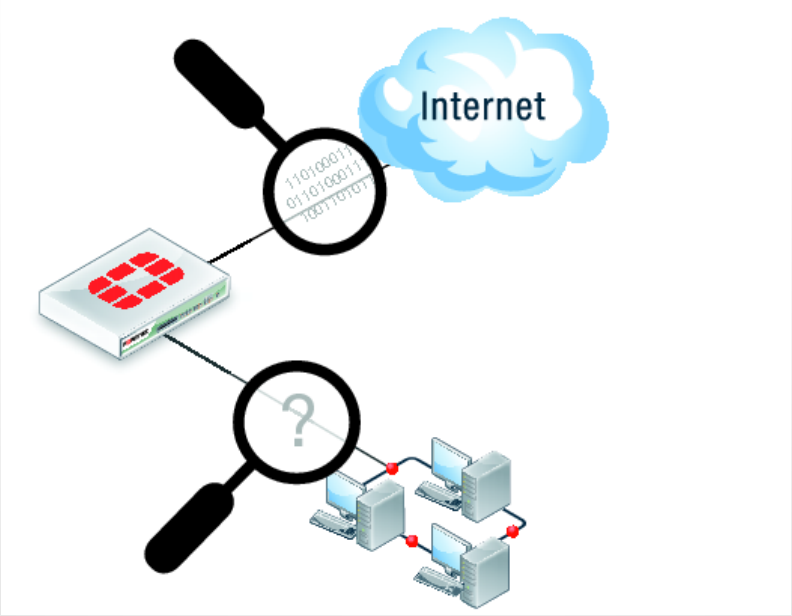
# Espionagem de Atividade Computacional por meio de Sniffers

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

# Espionagem de Atividade Computacional

O significado de espionagem consiste na prática de obter informações de caráter sigiloso relativas ao alvo sem sua prévia autorização esta é realizada sobre os dados armazenados em disco rígido ou sendo enviados ou recebidos através da rede.



# Espionagem de Atividade Computacional

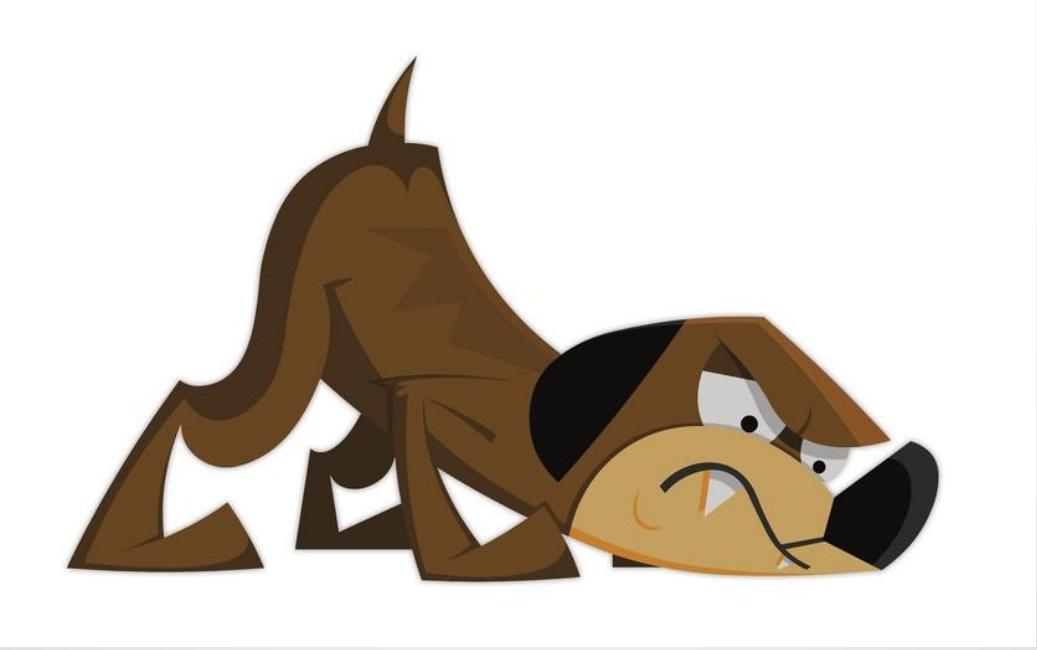
Seria espionagem apenas quando é feito um acesso externo à rede alvo?

Poderia o monitoramento de um gerente de rede ser considerado espionagem?

# Sniffers

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

Sniffers podem ser de Software ou de Hardware.



# Sniffers de Software e de Hardware

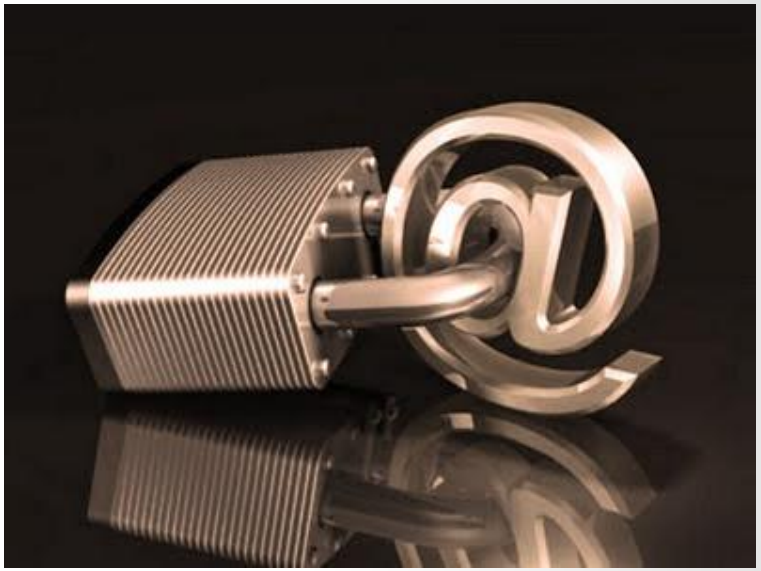
No *sniffer* por software, uma aplicação é instalada diretamente no alvo ou em um outro sistema externo responsável por fazer o grampo.

Por hardware, um dispositivo físico é acoplado no meio onde a informação trafega capturando os dados dos pacotes.

# Como Ocorre a Espionagem?

- Existência de 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;
- Simplesmente por diversão/curiosidade.

# Quais as Implicações?



- Criptografia
- Leis
- Caso Google Street View

# 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. Esse protocolo foi construído com o objetivo de prevenir esses tipos de ataques.

Ainda assim, podem-se realizar ataques **man in the middle** e de **replay**, já que ainda há a captura do pacote.

https://www.eff.org/de/secure-messaging-scorecard

# Leis

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.”

No Estados Unidos, também existe uma lei 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.

# Caso Google Street View

Segundo uma notícia publicada em 2011, o Google poderia ser investigado por interceptar, sem autorização judicial, dados privados de redes sem fio brasileiras.

As interceptações aconteceram entre 2009 e 2010, durante o levantamento de dados para o Google Street View.

Afirmam 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, incluindo dados privados de usuários.

# Caso Google Street View

Respondendo a acusação, a empresa admitiu que seu veículo interceptou redes sem fio, mas alegou só ter acessado redes públicas.

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.

# Caso Google Street View

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.

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.

# 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.

A realização de espionagem de atividades computacionais por meio de sniffing é considerada crime, se realizada sem ordem judicial. Somente analisando cada caso de espionagem pode-se julgar se foi ético e moral ou não.

# Bibliografia


Lei Brasileira

http://www.planalto.gov.br/ccivil_03/leis/l9296.htm

Acesso em: 18 de março de 2015

Lei Americana

http://communications-media.lawyers.com/privacy-law/wiretapping.html

Acesso em: 18 de março de 2015

Caso Google Street View

http://www.leieordem.com.br/google-pesquisador-cearense-acusa-o-street-view-de-interceptacao-de-dados.html

Acesso em: 18 de março de 2015

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