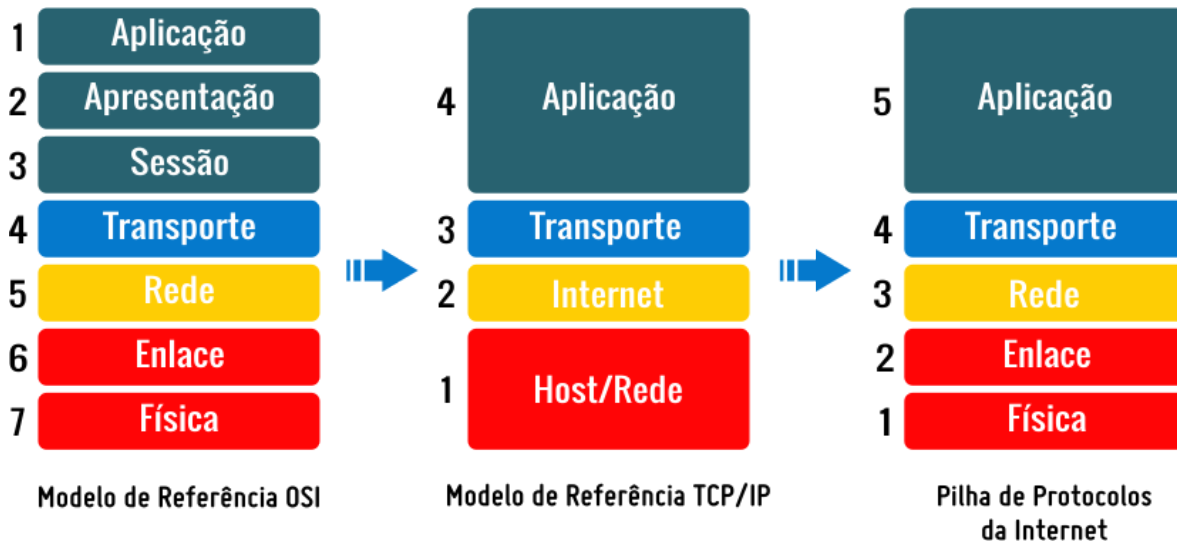




Segurança de Redes 1



Protocolo IP (camada de rede)

Não há garantias de entrega nem garantias de recuperação de uma mensagem. Pacotes podem se perder, ser permutados ou repetidos.

Se aplicação quer alguma garantia, esta deve ser aplicada na camada de transporte.

O ponto é que como sabemos se o pacote realmente veio de um endereço ip específico? Qualquer pessoa pode enviar um pacote afirmando ser um determinado endereço quando na verdade não é. *Não garantias de nada.*

Comunicação na internet

A comunicação dentro de uma rede local é feita com base em *MAC addresses*.

Tipos de ataque

Wiretapping

O wiretapping (grampo) é uma forma de escutar a comunicação de terceiros num canal de comunicação. O **wiretapping** pode ser:

- **Passivo:** a pessoa apenas escuta a comunicação. Isto é feito em alguns países.
- **Ativo:** quando o atacante injeta pacotes na transmissão.

Eavesdropping /packet sniffing

É uma forma de wiretapping em redes de comunicação, onde se recolhem e armazenam os pacotes trocados entre os utilizadores legítimos da rede. O Wireshark, por exemplo, é uma ferramenta que permite este tipo de ataque. Foram na verdade para serem usadas por técnicos da área.

Russian agents inspect undersea cables in Ireland amid fears they could tap into or tamper with links to US

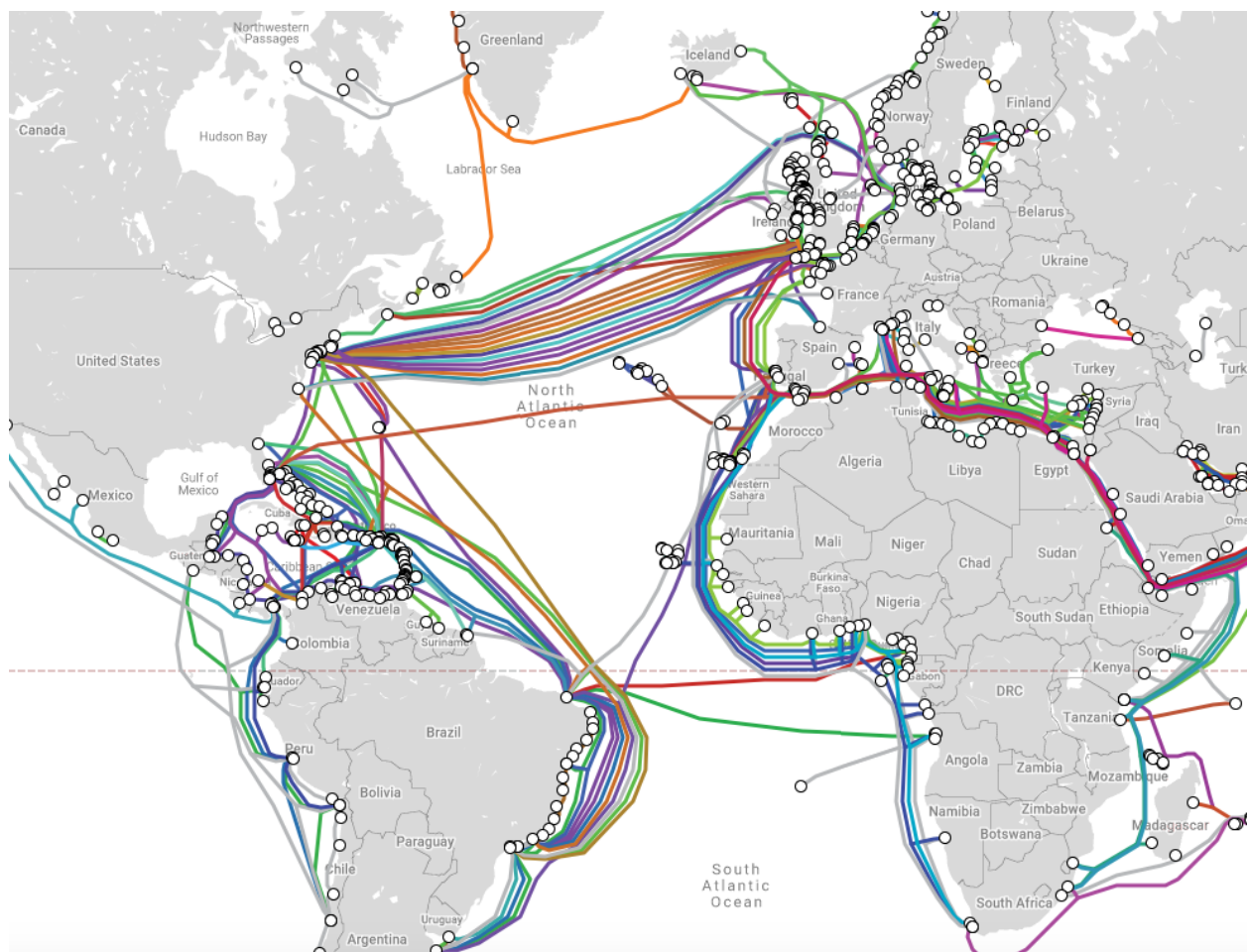
Since the reports, there's been widespread fear that the cables could have been tampered with or even completely cut. The cables in question are underwater fiber-optic cables which carry internet signals from North America to Ireland, the UK and mainland Europe.

<https://www.irishpost.com/news/russian-agents-inspect-undersea-cables-ireland-amid-fears-tap-tamper-links-us-179836>



In february 2020 have inspected the cables in ireland to check if US has not been tapping the communication.

In fact there're many cables in the world and tapping these connections isn't hard for a country with money and a motive.



Things became more visible with Snowden revelations. For example, the US National Security Agency was tapping the webcams from people in Yahoo.

Optic Nerve (GCHQ) - Wikipedia

Optic Nerve is a mass surveillance programme run by the British signals intelligence agency Government Communications Headquarters (GCHQ), with help from the US National Security Agency, that surreptitiously collects private webcam still images from users while they are using a Yahoo! webcam application.

W [https://en.wikipedia.org/wiki/Optic_Nerve_\(GCHQ\)](https://en.wikipedia.org/wiki/Optic_Nerve_(GCHQ))

MAC flooding: o melhor sniffing

Hoje em dia as redes em sua maioria são gerenciadas por switches. Se injetarmos mensagens com endereços MAC novos na rede, o switch irá esvaziar sua tabela de MACs e então irá começar a retransmitir todos os pacotes em broadcast.

Assim tem-se um sniffing mais eficaz.

MAC spoofing

Quando fazemos sniffing de pacotes podemos conseguir o endereço MAC de outro computador. Desta forma um atacante mudar o endereço MAC da sua placa de rede e começar a receber os informação como se fosse o algo. Isto só é possível, porque não há nenhum tipo de autenticação ao nível da camada lógica.

ARP poisoning/spoofing: usurpar IP

O protocolo ARP permite traduzir endereços IP para endereços MAC. Quando uma máquina não sabe qual o endereço MAC de outra, envia-se um ARP em broadcast e se a outra máquina estiver a escuta ela responde com o seu endereço IP.

O facto de switches poderem fazerem cache dessa informação faz com seja possível usurpar IPs. Inunda-se a rede com respostas ARP e em que se associa o nosso endereço MAC ao endereço IP dos que nos interessam.


Isto permite fazer com que atacantes façam o man-in-the-middle. Convince-se nós legítimos que a nossa máquina está associada ao IP do interlocutor. Isso implica que os pacotes de outra pessoa serão enviados para a nossa máquina.

Lemos, processamos e depois enviamos para o MAC certo, para que ele não detecte o que está a acontecer.

Hijacking de routing

BGP Hijacking In Iceland And Belarus Shows Increased Need for BGP Security - Internet Society

Want to understand better why we need to secure the Border Gateway Protocol (BGP) to make the Internet's routing infrastructure more secure? Just read this article on Wired's site, "Someone's Been Siphoning Data Through a Huge Security Hole in the Internet", or the corresponding post on the Renesys blog, "The New

 <https://www.internetsociety.org/blog/2014/02/bgp-hijacking-in-iceland-and-belarus-shows-increased-need-for-bgp-security/>



ICMP permite a descoberta de um router na rede. IRDP spoofing é anunciar um router falso. O atacante faz com que máquinas dessa subnet passem a utilizar o router inserido.

Rogue DHCP

DHCP intruso - Wikipédia, a enciclopédia livre

Um DHCP intruso é um servidor DHCP em uma rede de computadores que não está sobre o controle administrativo dos responsáveis pela rede. Ele é um dispositivo de rede, como um modem ou um roteador, conectado à rede por um usuário que não esteja ciente das consequências ou que esteja

W https://pt.wikipedia.org/wiki/DHCP_intruso?wprov=sfti1



O protocolo funciona da seguinte forma:

- O cliente faz um anúncio de que precisa de um IP.
- O servidor responde com uma proposta de endereço IP.

- O cliente lê a proposta e diz se aceita ou não o endereço IP.
- Quando existem vários sub-redes um agente DHCP pode servir de intermediário para falar com o servidor DHCP.

Um rogue DHCP server pode convencer um cliente de que o router/gateway está num endereço IP controlado pelo adversário. Isto permite um ataque man-in-the-middle.

Se o DHCP intruso fornecer como rota padrão (*gateway*) o endereço de uma máquina controlada por um usuário malicioso, é possível que este usuário tenha acesso aos dados enviados pelos clientes para outros computadores, violando a segurança da rede e comprometendo a privacidade do usuário.

DNS spoofing

Nada é autenticado aqui. É possível que um hostname nos direcione para uma máquina diferente. Esta troca pode ser feita por meio de um malware ou até mesmo quando se usa um servidor DHCP malicioso.

DNS(cache) poisoning (Kaminsky Attack)

É bombardear o servidor DNS local com respostas de resolução DNS.

Faz-se brute force aos parâmetros conhecidos na pergunta DNS (query ID)

O servidor aceita a proposta que contém o IP controlado pelo atacante.

O servidor DNS local informa máquina do utilizador com o IP errado.

Perguntas

1) O que é wiretapping?

▼ Resposta

O wiretapping é a prática de se escutar a conexão de outros utilizadores autenticos na rede. O wiretapping pode ser **passivo** onde a pessoa apenas escuta a transmissão e não interfere nela. No tapping **ativo** o atacante injeta pacotes na rede.

O wiretapping pode ser feito diretamente em cabos.

2) Por que MAC flooding é considerado o melhor sniffing?

▼ Resposta

Porque quando inundamos a rede com mensagens de endereços MAC a tabela do switch pode ficar cheia. Quando isto acontece, o switch passa a fazer broadcast das mensagens que devem ser transmitidas. Assim o atacante pode passar a escutar e/ou roubar pacotes.

3) É possível o atacante roubar o endereço MAC de alguém e aproveitar este facto para roubar pacotes. Qual o nome do ataque?

▼ Resposta

MAC spoofing

4) O que é ARP spoofing?

▼ Resposta

O protocolo ARP é responsável pela resolução do endereço MAC de alguém. O switch envia um ARP para a network em broadcast e quando a pessoa responde salva-se na tabela o endereço MAC correspondente ao endereço IP.

O ARP spoofing consiste em inundarmos a rede com respostas do protocolo ARP em que se associa o endereço IP da vítima ao nosso endereço MAC. No fim isto funciona como um man-in-the middle.

5) O que é rogue DHCP?

▼ Resposta

Este é um protocolo de resolução de endereço IP. O DHCP envia para o computador uma proposta de endereço IP. A máquina recebe a proposta e responde se aceita ou não. No entanto, em sub-redes pode acontecer de se ter um agente DHCP que redireciona a mensagem para o DHCP. O atacante pode convencer a pessoa a se conectar ao DHCP controlado pelo atacante.

6) Como é possível realizar o DNS spoofing?

▼ Resposta

Um atacante pode alterar a tabela de DNS de uma máquina qualquer de forma que um host redirecione para um endereço IP comprometido. Isso pode ser feito por meio de malware ou até mesmo quando um atacante controla o DHCP.

7) Qual a diferença entre DNS spoofing e DNS poisoning?

▼ Resposta

O DNS poisoning consiste em inundar a rede com mensagens de resolução de DNS. Por brute force um servidor pode aceitar a resolução do DNS. Depois quando o user tentar acessar o website o servidor DNS fornece o endereço IP errado.