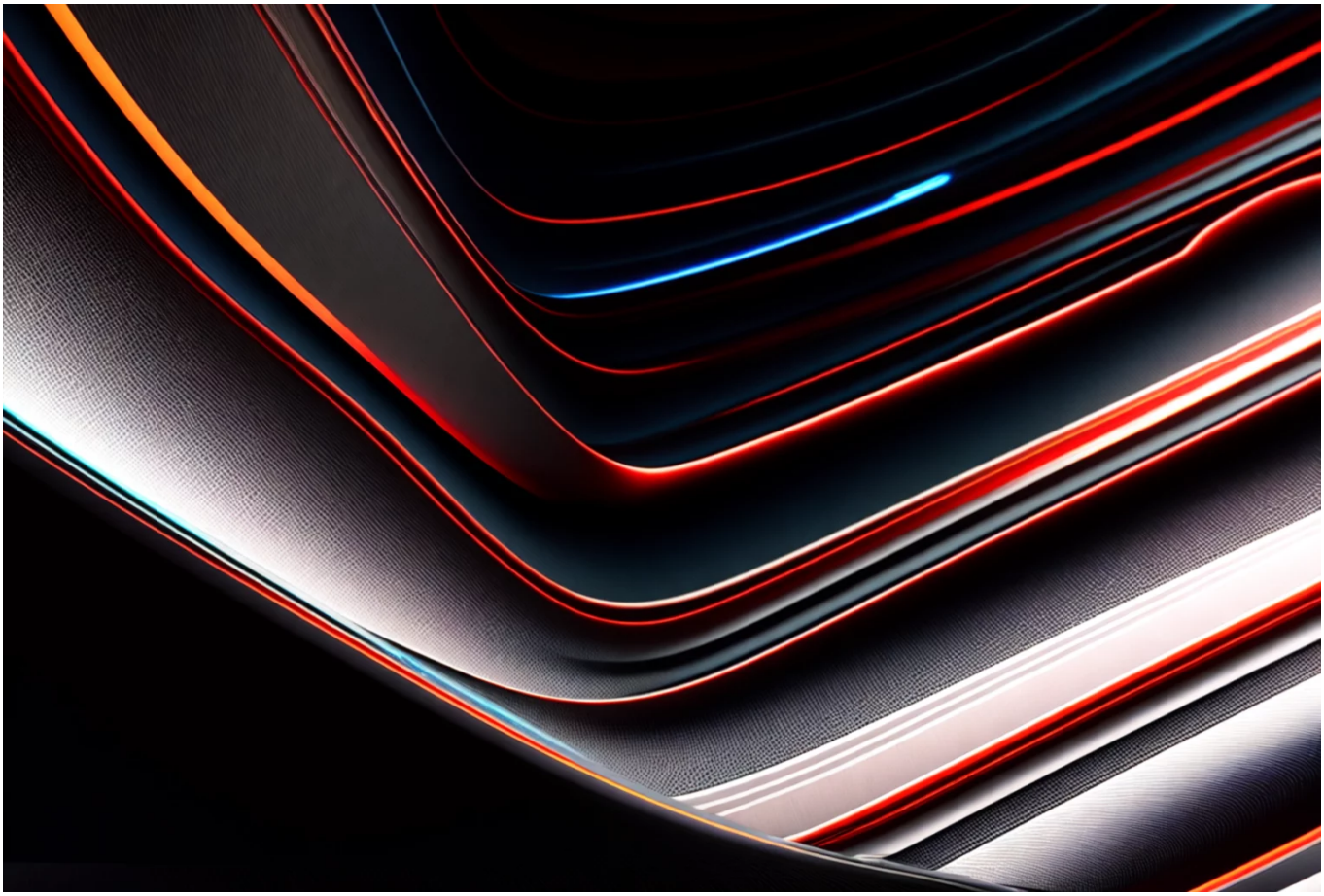
(https://mercurysnotes.com/)

What is a Quantum Insert Attack?

Daniel Iwugo(https://mercurysnotes.com/author/elementmerc/)
August 14, 2023(https://mercurysnotes.com/2023/08/14/)
Read Time: 3 mins



Abstract v3 ¦ Credit: Mercury (https://www.pexels.com/@mercury-el-598575147/)

I listened to a recent episode of Darknet Diaries (https://darknetdiaries.com/) (great podcast by the way) where the host, Jack Rhysider, talked about Operation Socialist. The operation (https://www.theguardian.com/uk-news/2018/sep/21/british-spies-hacked-into-belgacom-on-ministers-orders-claims-report) was a campaign allegedly carried out by the United State's NSA and Britain's GCHQ to hack into the one of the biggest telecommunication organisations in the world, with the aim of information gathering.

It was also alleged that one of the techniques used for the hack was also used against OPEC but that's a story for another day. However, we're going to look at the technique that was used to carry out these operations: The infamous Quantum Insert.

Prerequisite Knowledge

Before you get your hopes high, no, it doesn't have anything to do with a quantum computer. On the other hand, it does require some fast paced computers. Before we get started, you'll need to first understand how your device surfs the Internet.

In order to carry out a Google search, send an email or take a picture to keep your Snapchat streak with your friends, you need an Internet enabled device. In a network, any can be classified as a 'Client' or 'Server'. Clients ask for resources while servers deliver them. So when you search for your favourite song, your 'Client' phone sends data packets to a Spotify 'Server', which in turn sends data packets back to your phone.

Now that you understand this, let's take it up a notch and look at how a QI (Quantum Insert) works.

How a Quantum Insert Attack works

The Quantum Insert Attack process is explained in the steps below:

1. **The attacker infiltrates and monitors network traffic**

   An attacker would gain initial access into the network and monitor the network traffic to see what could be of interest and will allow for the best chance of success. For example, keeping track of what websites are commonly visited by the victim.

2. **The attacker sets up a *Shooter* and waits**

   A Shooter is a high-speed malicious server with very fast response times. The attacker programs the shooter to send a response to the victim when certain

conditions are met.

3. **The victim requests resources from a server**
   The victim would visit a website that matches the set conditions for the shooter to respond to. In contrast to similar attacks, QI is a Man-On-The-Side attack. This means it can't modify or delete packets, but can read and inject packets in the data stream.

4. **The data packet for the request 'splits'**
   The word 'split' should be taken with a grain of salt. However, it relays the idea that the request packets from step 3 are sent to both the server and the shooter.

5. **The shooter sends a response back to the victim**
   The shooter quickly responds to the victim by sending a malicious version of the resource requested. For example, a malicious webpage. The actual response packets from the legitimate server are received but dropped because the computer thinks it already has what it asked for.

Mitigations

The researchers at Fox IT have some suggestions (https://blog.fox-it.com/2015/04/20/deep-dive-into-quantum-insert/) on this:

1. **Use HTTPS along with HSTS**
   HTTPS is the secure version of the common protocol used to communicate over the Internet. HSTS (HTTP Strict Transport Security) is a policy that ensures HTTPS is implemented properly. Although not fool proof, using the combination of these two can reduce the effectiveness of QIs.

2. **Use a CDN with low latency**
   A CDN (Content Delivery Network) allows for web resources to be delivered to users faster. Having one with low latency (high speed), could make the

legitimate packet win the race to the victim over the malicious one.

3. **Configure your IDS with some new rules**

   There are two anomalies when a QI occurs. First, the sequence numbers of the response packets from both the shooter and legitimate server are the same. Secondly, the TTL (Time to Live) values of the packets are different. Both can be detected with a properly configured IDS (Intrusion Detection System).

(https://mercurysnotes.com)