Cyber-Security Myth

Introduction

Although the Internet has made phenomenal advances during the last few decades, it remains fragile and vulnerable to attacks large and small to this day. Users are confused as to its convoluted workings and are often unable to distinguish between a hack by an intruder and a break in the protective software.

One such recent event occurred on 2025 November 18 when Cloudflare suffered a global outage that briefly broke a huge slice of the internet. This was not an isolated incident. The previous one happened only eight months prior, and there were more before that. Similarly, Amazon Web Services (AWS) has been disrupted frequently. This kind of Internet outage has become almost routine and the reliability of these services designed to defend against cyber intrusions has come into question.

The Problem

The Internet's vulnerability has been an issue for decades. Last year, the Federal Communications Commission (FCC) issued a Notice of Proposed Rule Making (NPRM) that identified the Border Gateway Protocol (BGP) as the target for mitigating the risk. The Internet Architecture Board (IAB), representing the Internet community, responded with a comment expressing concerns. Nevertheless, the White House published a Roadmap which focused on the BGP integrity as the means to enhancing Internet routing security.

In this regard, it is important to bear in mind that the BGP is required to transport packets between Autonomous Systems (ASes) that are selected by the Domain Name Server (DNS), based on IPv4 addresses assigned to subscribers by the Dynamic Host Control Protocol (DHCP), which was created to deal with the IPv4 address shortage. This protocol stack has resulted in a complex system architecture vulnerable to attack from many angles, each requiring another patch in response.

The Solution

A flawed system invites a never-ending series of hacks and patches. A much more robust Internet can result from a simplified and streamlined architecture that eliminates the root-cause of IPv4 address shortages, thus negating the need for any of the above-mentioned four protocols. Such is the result of a deterministic system dubbed EzIP.

(Please visit https://avinta.com/gallery/CyberSecurityMyth-US.pdf for full text.)