AA-Consulting

WHITE PAPER

LAYER 1 SECURITY

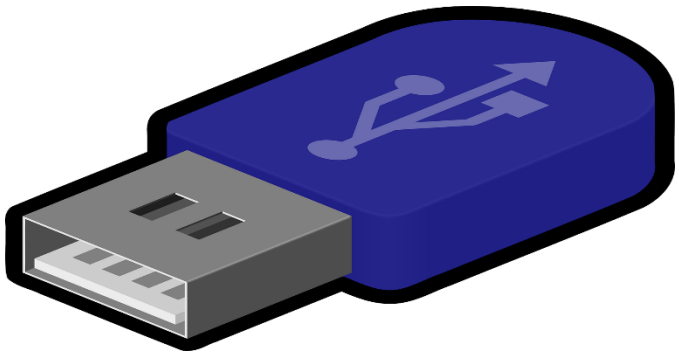
Nowadays, more focus is put on applications. As a matter of fact, existing security solutions such as NACs, IDS and IoT network security are traffic-based and do not cover the physical layer of the OSI model. They simply lack layer 1 visibility. Without a clear insight, there exists a blind spot to the physical specifications of the network infrastructure of organizations. Such blind spots results to rogue devices being undetected, and spoofing devices getting recognized as legitimate devices, thus exposing the enterprise to harmful attacks.

The physical layer (layer 1) is the lowest layer of the OSI model that is responsible for identifying the physical equipment involved in data transfer. Layer 1 defines the relationship between a device and the medium used for transmission. This includes the layout of pins, cable specifications, hubs, repeaters, etc.

Do you Know all the physical devices connected to your network right now? Remember, you can't actually secure what you don't know you have!

AA-Consulting

WHITE PAPER



Through this layer, information is usually transmitted from one physical node to another in the form of bits. Being the first of the OSI layers, it is of extreme importance to ensure sufficient physical level security at layer 1 in order to prevent imminent attacks.

Due to the complexity and size of the network infrastructure in many organizations, these organizations are blind to a bulk percentage of the assets connected to their network; assets from BYOD and remote work inclusive. This blind spot leaves them unaware of the ever-increasing vulnerabilities that lie within their asset surface area, meaning that risks remain uncontrolled with a greater susceptibility to rogue devices, service disruptions, compliance breaches and other damages that may arise from failure to manage asset risks. As a matter of fact, it remains a problem to ensure efficient physical layer security when you don't precisely have a full visibility of the whole assets connected to your network.

As Physical layer is the first layer of the OSI model, it is imperative to have a full visibility of all connected devices in order to get defenses in place and reduce impending layer 1 risks

When all devices within an enterprise are effectively detected, that enterprise benefits from a detailed and overall cybersecurity posture. Sepio's Hardware Access Control (HAC-1) Solution has been specifically built to understand what you have connected in the physical layer, while gaining full visibility of all the hardware devices ranging from endpoint peripherals to connected devices (IT/OT/IoT). Using its out of box management interface, Sepio uses layer 1 information like impedance, voltage, noise, etc. that are specific to devices to build fingerprints for each device. Sepio leverages this fingerprinting approach to identify all physical devices connected on the network since every device has a unique fingerprint associated with it.

To learn more about the neglected area of layer 1 security, and to see a demo of how Sepio discovers all the physical assets connected to your network, reach out to us at AA-Consulting. We are a top partner to different renowned vendors of security solutions, Sepio layer 1 security solution inclusive.

ABOUT AA-CONSULTING

Headquartered in Israel, AA-Consulting established its regional offices in Lagos, Nigeria in 2001. The company specializes in IT services to local organizations and companies. This includes local technical staff of experienced engineers and high-level customer service and support.

Our solutions are based on advanced technologies, backed by a team of skilled and experienced customer support engineers. The company had excelled in local representation for over a decade, providing fast response time, problem solving and readily available products.

AA-Consulting

www.aa-consult.com

Hachayil 43
Ramat-Gan
Israel
+972 (77) 5510082

No. 334 Ikorodu Road,
Anthony, Lagos
Nigeria
+234 (806) 5588717