Air Gap Usage And Methodology In Data Protection

Air Gaps are a well-established best practice in cybersecurity and the only known generally impenetrable protection for critical data or systems.

Unfortunately, the high degree of security provided by a properly implemented air gap comes at the expense of convenience and ease of use since a physical disconnection of a device or network segment must be made whenever the air gap is opened or closed to access or protect data respectively.

For this reason, air gaps to date have generally been either underutilized or implemented in an improvised fashion which is insecure. A common practice in many data centers is to emulate an air gap utilizing virtual LAN (VLAN) capabilities in switching or routing hardware. VLANs utilize traffic segregation at the data layer (layer 2 of the OSI model immediately on top of the physical media layer) between ports to isolate traffic on one port or group of ports from another. This emulates the functionality of an air gap with one crucial flaw: the data is still traversing the same physical layer. As such, if the switch or other device carrying the traffic is compromised, the segregation of data is easily breached and all data security is compromised. This is a common occurrence where VLANs are used to protect critical data or network segments. As such, a VLAN emulation is NOT equivalent to an air gap for security and, in reality, is little better than no additional protection whatsoever.

The EtherGap™ (patent pending) was designed to resolve this specific issue. The EtherGap™ contains two separate physical layers. One layer connects or disconnects target devices or networks from each other by implementing a physical air gap between them controlled by electromechanical relays. The other layer, completely physically isolated from and unreachable by the first, carries only control signals for a microprocessor which generates signals to open or close the electromechanical relays which operate the air gap. If an attacker breaches the user's LAN from the Internet, they still cannot reach data protected by the EtherGap™ because it's controls cannot be operated from the Lan.

This methodology - out of band control signaling - allows for a controllable air gap which is impossible to compromise from the protected network, associated LAN or WAN. It is similar in operational principal to the solution implemented by the Bell System some time ago where in-band signaling to route and connect phone calls was removed from the voice band to thwart "blue boxing" and other similar methods of subverting the controlling systems via in-band signals generated by unauthorized users and devices. Control of the system was moved to completely external wiring and processors on a separate physical layer from the layer carrying the traffic and ended the security issue.

EtherGap™ control signals can be initiated in numerous ways. In attended data center operation, an operator can simply open or close the air gap by touching the touch screen controls on the front of the rack mounted device or do so remotely over a hardwired (isolated not exposed to LAN nor WAN) admin network connection. The device also has an internal WiFi access point for direct encrypted access via devices which are not concurrently connected to other networks. (A "remote control" model.)

A timer signal is another common operating method. The EtherGap™ can be programmed to open or close the air gap at a specific time and remain in that state only long enough for a specific operation to complete. An example would be backups of a system. A backup storage device would normally be isolated from the LAN by the EtherGap™ since that LAN is connected to the Internet (WAN) and thereby at risk. At a predetermined time, a programmed script on the EtherGap™ or a system protected by it would first disconnect the LAN from the Internet (WAN) and then connect the backup storage to the LAN. Backups are then copied from targets on the LAN to the backup storage. When complete, the EtherGap™ returns the backup storage to isolated state (gap open) and the LAN Internet connection to connected state (gap closed). In this manner, the backup drives are never exposed to attack from the Internet as they never connect to each other. Programming the backup device or EtherGap™ itself to "pull" the data further reduces the attack profile from the LAN side by maximizing defilade of the backup drives and EtherGap™ itself. Because the EtherGap™ has 3 RJ45 network ports in a standard configuration (Common, Normally Open, and Normally Closed) this isolation gap methodology can be done with a single operation.

As cyber threats continue to multiply and spread, air gaps will become the standard in data protection and the EtherGap™ will be at the forefront of their implementation and use.

ETHERGAP

Michael Voss
Founder and CEO
EtherGap Systems
3435 Ocean Park Blvd. Suite 107661
Santa Monica, CA 90405

(310) 651-5235
voss@ethergap.com
www.ethergap.com