EVERIS

The Cornerstone of Network Security

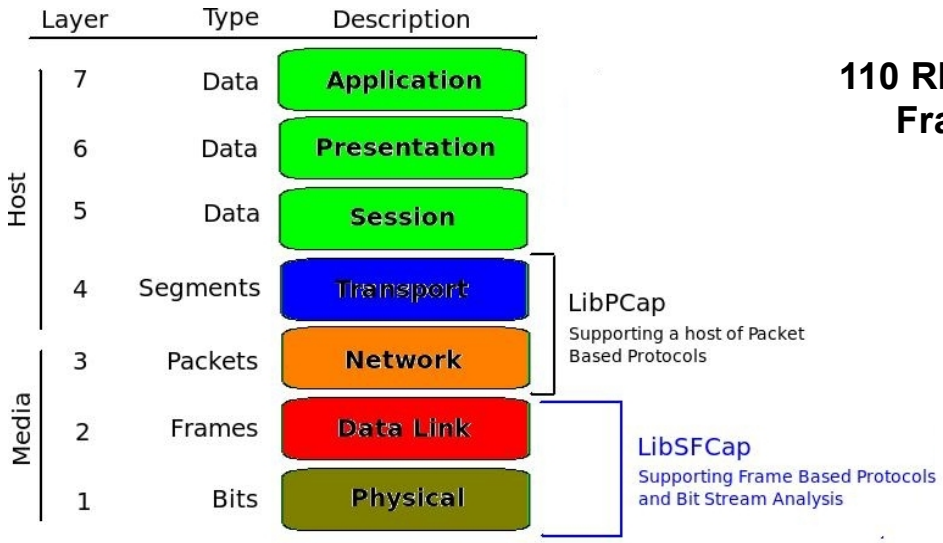
Hammerhead

A 7 Layer Holistic Solution For Cyber-Warfare

Hammerhead Platform

Is the first true 7 Layer network security platform. It was designed as part of Everis's Cyber Operations for Optical Networks (CyOON) toolkit. Hammerhead it's self uses a 7 layer approach to analyzing and managing traffic. In the past network security monitoring has been limited to only layers 3-7 of the OSI reference model due to their reliance on protocol analysis libraries and tools such as LibPCap.

Everis's efforts have resulted in a number of tools such as LibSFCap which has become the foundation for the CyOON toolkit. Not unlike LibPCap, which a number of applications; most notibly SNORT, TCPDump, and Kisment are built on, LibSFCap is a protocol capture library with the distinct difference of being specially built to analyze traffic from Layers 1 and 2.



Everis Inc
110 RR Street, Suite 11
Frankfort NY, 13340

(315)-370-1535

EVERIS

The Cornerstone of Network Security

As LibPCap was instrumental in a change of the IP Security Landscape, LibSFCap will be for the Optical IA Landscape. The LibSFCap API can be used in any program to capture the optical bit stream and and break it down into it's individual SONET frames at near-real-time and produce output in a more comprehensible form.

This is done through a comprehensive understanding of how SONET is formed and broken down by intermediate WAN Nodes. LibSFCap breaks down both the header and SPE (Synchronous Payload Envelope) into their individual components and provides them as output. The API can be set to give all or only a few items out at a time based on what the user asks it to.

Software:

The Hammerhead platform was designed with threat detection and mitigation in mind. It includes something for all areas of WAN Security including:

- WAN Level Spoof Detection (Patent Pending)
- WAN Flow Control for DdoS Mitigation (Patent Pending)
- The OISF Network Intrusion Detection System
  - This is the future of NIDS, The OISF NIDS is a first generation SNORT replacement that supports multi-threading, preprocessors and multiple protocol interpreters at speeds well beyond anything currently available.
- Stream Based File Extraction (Everis Developed Software)
- SGUIL and BASE NIDS Frontends
  - Both Front Ends have been modified specifically for use with the OISF NIDS and LibSFCap
- NAGIOS and P0f for Network Inventory and System Identification
- SysLog and ArchSight Integration for Network Management
- Argus for Asset Management
- A Deep Packet Solution (Everis Developed Software)
- and many more …....

The box is designed in such a way as to be deployed as either an in-line or out-of-band solution and the software has been modified as such. Allowing for you to deploy it in in high speed operating environments with up to 4 x 10 Gbps SONET/PoS/IPoS/EoS per box as an NSM , or 2 x 10 Gbps Connections in and 2 x 10 Gbps Connections Out as a Gateway.

EVERIS

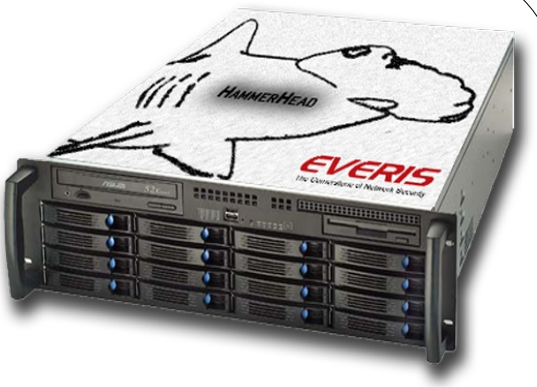
The Cornerstone of Network Security

Hardware:

System Specifications:

The CyOON Hammerhead comes laoded in it's default configuration with the following, though additional configurations can be customized based on your needs:

- 24 x 2.6 GHz Cores
- 64 GB DDR 2 RAM
- 2.1 TB of SAS Storage
- 18 TB of SATA Storage
- 4 x 1 Gbps Coper Network Interfaces
- 4 x 10 Gbps Optical Network Interfaces



Capture Card:

The Endace® DAG 5.4SGA-48 network monitoring card provides the flexibility to capture and inspect traffic on multiple network types, including OC-3/12/48c/OC-192 (STM-1/4/16c) Packet-Over-SONET(POS) and 10/100/1000 Ethernet and RAW Mode which Enables Everis's LibSFCap. Hardware packet processing enables sustained line rate traffic classification, and filtering prior to transfer to host system memory via the PCI-X bus. Coupled with an efficient interrupt-free and zero-copy DMA data path directly from the card to application software, the DAG 5.4SGA-48 empowers solutions to scale to multi-Gigabit performance. With precise packet time-stamping to nanosecond resolution, complete visibility is provided into network behavior.

endace

power to see all