Executive Summary:

Changing the Economics of Lossless Full Packet Capture Enabling Real-time Visibility

March 2017

All questions and enquiries regarding this white paper should be directed to:

Dan Cybulski
Chief Technology Officer
dan@cognitiocorp.com

Table of Contents

Background

Federal organizations have mandated requirements to keep users and data safe. Data integrity, user access, and application security are the key ingredients to fulfilling these security requirements. However, computer networks at federal agencies and departments today are both more complicated and mission critical than ever before. Despite continued efforts to collapse networks and consolidate programs across agencies, data classification and compartmentalization has driven the creation of complex sets of enterprise and mission networks. These isolated, and carefully interconnected networks are necessary to enforce data security and need-to-know policies in pursuit of mission objectives. Still, managing, monitoring and securing these networks remains an ever-evolving challenge for these agencies.

Packet capture (PCAP) and capture-to-disk (C2D) are some of the most fundamental capabilities employed by agencies to address the challenges of operating and defending their vast and complicated networks and IT infrastructure. A mechanism for intercepting data packets that are traversing a computer network, effective PCAP/C2D systems can provide administrators, engineers and executives with an accurate, real-time view of what is happening within a network. These capabilities can be deployed within an organization to monitor for security events, identify data leaks, analyze network performance, troubleshoot issues, and even to perform forensic analysis to determine the impact of cyber-attacks and network breaches.

Today's packet capture systems are comprised of two major components: a mechanism for capturing the packet data, and an analysis capability to review the captured traffic. While much of the emphasis is put on the analysis capabilities, this is of little use without a high-fidelity capture solution capable of keeping pace with today's high speed networks. This paper will discuss the options that agencies have in the capture space and highlight how solutions from Solarflare® can provide agencies with high-fidelity capture capabilities, including high-speed capture-to-disk and real-time analysis of network flows.

Value to Mission

Large complex technical organizations need to understand how their user base, applications, data, network, and security interact and coexists. These environments are ever-changing, requiring instrumentation, metrics, and analysis from highly capable tools to provide this visibility.

The Solarflare SolarCapture platform combines industry leading network adapter technology with intuitive software to simplify deployment and management while enabling real-time analysis of network flows and packet data. SolarCapture provides unmatched flexibility, through its open platform, enabling multiple deployment options and third party integrations to power:

High-speed Capture and Replay

The SolarCapture platform enables lossless capture-to-disk at 1/10/40 Gbps speeds. Leveraging the custom ASIC technology and kernel bypass capabilities inherent in Solarflare's network adapter, SolarCapture keeps up with the performance of the highest speed networks while enabling precise timing and inter-frame gap control for the most demanding capture requirements.

Disaggregation of Capture and Analysis

SolarCapture is designed as an open platform focused on enabling new, real-time analysis capabilities without sacrificing existing analysis capabilities. This is achieved by disaggregating the capture and analysis systems, allowing for seamless integration with third-party analysis tools.

Simultaneous Query and Capture

SolarCapture is specifically designed to perform line-rate packet capture and indexing to provide expedited retrieval of captured traffic without impacting the performance of ongoing capture. This enables real-time analysis of active capture data.

Technical Approach

Capture-to-disk solutions are a key tool empowering agencies to measure performance, identify bottlenecks, troubleshoot issues, and secure enterprise and mission networks. Today, most agencies leverage commercial capture-to-disk appliances to meet their needs, while some choose to create their own solutions (DIY) from off-the-shelf network adapters and open source software tools. While each of these approaches have strengths they also have inherent limitations that make them suboptimal for todays high-speed and ultra-scale network environments.

Conventional Commercial C2D

Commercial capture solutions have historically been the go-to solution for large and small enterprises as they look to instrument their networks for greater visibility and improved security. These products typically come in the form of an appliance, which appeals to many organizations in search of plug and play solutions. The deployment and management simplicity of these appliance based solutions is often considered to be the most significant benefit over the DIY alternative. However, this approach also has some major limitations:

- Lack flexibility
    - Traditional appliances provide limited deployment flexibility.
- Utilize proprietary data formats
    - Proprietary data formats limit the integration of third party tools, constraining analytic capabilities and diminishing long-term forensic value.
- Lack integration with cloud for hybrid environments
    - Existing commercial solutions have been slow to adopt cloud and hybrid architectures making it difficult to leverage cloud for long term storage and post capture analysis.

In addition to the above challenges, the closed source nature of most commercial capture solutions carries economic disadvantages. While often based on commodity platforms, these capture solutions frequently incorporate special purpose components to achieve capture performance. These components increase cost and complexity while limiting the organizations ability to leverage existing investments in storage and analytics platforms. Moreover, this proprietary approach limits the organizations ability to incorporate future technology enhancements (i.e. NVMe).

Do-it-Yourself C2D

The drawbacks of commercial capture solutions have driven some enterprises to invest time in creating their own capture capabilities using off-the-shelf hardware and open source or commercial driver software. The significant advantage here is in flexibility. The use of open source software and off-the-shelf hardware results in a more open platform that allows data to be analyzed both in near-real-time and exported in an open format to long-term storage to support future forensic analysis and replay. However, this approach too has some major limitations that must be addressed:

- Deployment difficulty
    - Despite the benefits of open source software, it requires significant engineering and development resources to deploy, manage, and integrate with existing capabilities.
- Performance challenges
    - None of the high performance open source or commercial solutions available include disk writing capability because it's an extremely tough balancing act. Writing to disk for a single 10GbE interface requires supporting 1.25GB/sec continuous throughput. While this might sound simple, few 2U or 3U servers with built in RAID arrays are capable of sustaining this level of performance. Once you add in the requirement to simultaneously support querying what has or is being written to disk these systems begin dropping significant volumes of packets.

C2D with SolarCapture

The SolarCapture platform from Solarflare harnesses the strengths of each of these approaches to address their limitations and deliver the best of both worlds. Based on Solarflares industry leading Ethernet adapter technology and software, SolarCapture provides lossless capture and indexing of network traffic at line rate with simultaneous query capabilities for real-time network visibility. The SolarCapture platform offers a number of key benefits over other commercial and open source solutions including:

- Flexible deployment
    - The SolarCapture family provides everything from turnkey appliances to network adapters and SDK's. The flexible deployment options support both the unique needs of bespoke mission environments and enterprise deployments alike
- Open platform
    - SolarCaptures SDK's and open API's allow for easy integration with third-party tools, analytic frameworks, and storage platforms. Furthermore, native integration already exists for many current analysis platforms (i.e. Splunk, Tenable, Hadoop).
- Cloud integration
    - SolarCaptures native cloud integration (including AWS) simplifies deployment in hybrid environments and enables low cost cloud storage to be leveraged for long-term forensic data retention.

In addition to these overall benefits, SolarCapture also provides centralized management and industry leading data compression to enable the efficient use of storage and seamless horizontal scale of capture capabilities in ultra-scale and deployed environments. The tight integration between hardware and software inherent in the SolarCapture platform provides unmatched lossless capture performance. Moreover, its open approach and cloud integration provide a flexible platform to support a wide range of deployment scenarios including mission specific capture and analysis of sensor data and other non-traditional capture data.

Summary

Gaining a real-time view of network operations and activities has become a critical capability for agencies as they seek to understand network performance, provide application visibility, and meet real-time monitoring and compliance requirements. As network speeds and bandwidth continue to increase across enterprise and mission environments they are beginning to out-pace the performance of traditional capture-to-disk solutions, making this level of visibility harder to achieve. Furthermore, these traditional solutions generally implement proprietary algorithms and data formats making it difficult or impossible for agencies to tune these platforms to meet their unique needs. However, SolarCapture from Solarflare provides agencies with an open platform that is flexible enough to meet the needs of both the largest enterprise wide deployments and bespoke mission deployments. SolarCapture, based on Solarflare's industry leading network adapter technology, provides lossless capture, storage and analytics of packet and flow data on even the most demanding, ultra-scale agency networks.