PROFITAP

Special tool for special forces

Tapping into real-time threats in the cyberspace

Cybersecurity – a rising challenge

Security is one of the biggest concerns today. Ever since the advent of the 21st century, the world has been facing several challenges regarding the security of people, economy, and infrastructure. One of the facets of the security concern in this new millennium, the digital age, is information security, often known as cybersecurity. The complexities of the physical security space have multiplied in the cyberspace due to sophisticated threat mechanisms and the ever evolving technological advances. Traditional crimes are now being vectored through cyberspace, ranging from public attacks, financial fraud, intellectual property violations, sabotage of critical infrastructure, compromise of security intelligence information, and even penetration into national defence communications. All of these bear significant human and economic consequences. As information technology is being integrated into the physical world increasingly, the risks of these consequences escalate every day.

Cyberspace is more difficult to secure than the physical world. The ability of malicious activities to originate from anywhere in the world, the integration of physical systems with cyberspace, and the possibility of new vulnerabilities arising in complex cyber networks are the key factors for this difficulty. Because of the scale of consequences possible in the cyberspace, Cybersecurity has now become an important mission for defence establishments, law enforcement agencies, and national security forces worldwide. This created a need to have special purpose technical teams within these agencies and forces to address the security concerns in the cyber arena. The range of operations of these teams varies: network security & defence, post-event forensics analysis, hacking & penetration, security intelligence & surveillance, and on-field threat defence, are the common domains.

Seeing beyond the network

In order to detect and counter security threats in the cyberspace, security teams need to be able to see beyond the usual level of network elements. They should have the ability to see through those elements and view the actual traffic running over the network. If they are able to analyse actual data packets flowing over the network, they can identify malicious data patterns and detect threats in real-time. To do that, a packet capture mechanism is required for intercepting and capturing packets from the live traffic.

There are two ways to capture packets: using port mirroring (SPAN), or, using a network TAP. The latter beats the former method by every aspect of performance and ability. Let's have a quick look at each of these methods.

Port mirroring, also known as Switched Port Analyser (SPAN) in the Cisco world, is a mechanism used on network switches to copy traffic from one port (source), or an entire VLAN even, to another port (destination) of a switch. A monitoring appliance or a packet analyser connected to the destination port would then receive the same traffic as seen on the source port. At first glance, port mirroring seems to be a convenient and inexpensive way to access traffic flowing through a network switch. However, port mirroring has serious implications when it comes to accuracy and performance. To begin with, one of the issues of using SPANs is that they do not provide the mobility to roam around various network locations for capturing packets during forensic analysis. Because there is no guarantee whether there would be a vacant port available to mirror the required traffic on the specific target switch. A bigger bottleneck is that the cybersecurity team would never be able to see each and every packet from the mirrored traffic

stream. Because SPAN ports cannot copy the traffic streams from all switch ports, which usually aggregate to more than the SPAN port's capacity, without dropping some of the packets (up to 50% in worst cases). On top of that, SPAN ports have the least priority in the switch's internal matrix. Thus, using SPAN fails the original purpose of the entire activity, i.e. to be able to capture and analyse all the packets in real-time.

The second, and more reliable, method to capture packets is using a network TAP (Traffic Access Point). A network TAP is a piece of hardware that is installed in-line on a network link. It creates an internal mirror of the traffic flowing over that network link without disrupting the original traffic. It also contains an internal bypass mechanism to keep the network link intact in case of any issue with the hardware itself (e.g. power).

A network TAP does not incur any of the bottlenecks involved in using port-mirroring. It can be installed at any network location over a network link of interest without having to do any configurations in any of the network switches. Because a TAP captures packets on the wire, it guarantees full capture of 100% of packets from the live traffic in real-time. TAPs are being used extensively in security applications because they are non-obtrusive and are undetectable on the network, having no physical or logical address. Thus, the cybersecurity team can execute their activity in complete stealth mode.

SWAT-style operations in the cyberspace

Special Weapons and Tactics, or SWAT, is a term used by law enforcement agencies to identify security units employing specialised equipment & tactics for handling threat defence and security operations by unconventional counterattack measures. It was first established in Philadelphia, United States, in 1964, by the local police department in response to an alarming increase in bank robberies. Unlike conventional responses to bank robberies, in which the police usually respond after the event is over, the main purpose of the SWAT team was to react rapidly to bank robberies while they were in progress. Thus, the prime objective of a SWAT force is to neutralise threats in real-time. Following the success of the SWAT force in United States, countries across the world have adapted to this style of counter-terrorism with their own local versions of SWAT, usually terming them as an elite force or special squad.

The key to a successful SWAT operation is choosing the right type of specialised equipment and deploying on-ground tactics based on the nature of threat event.

To support cybersecurity teams for their own SWAT-style operations in the cyberspace, there has to be a tool which enables them to counter and neutralise threats in real-time. Considering network TAPs to capture and analyse live traffic packets, the SWAT-style tool should have the following key characteristics.

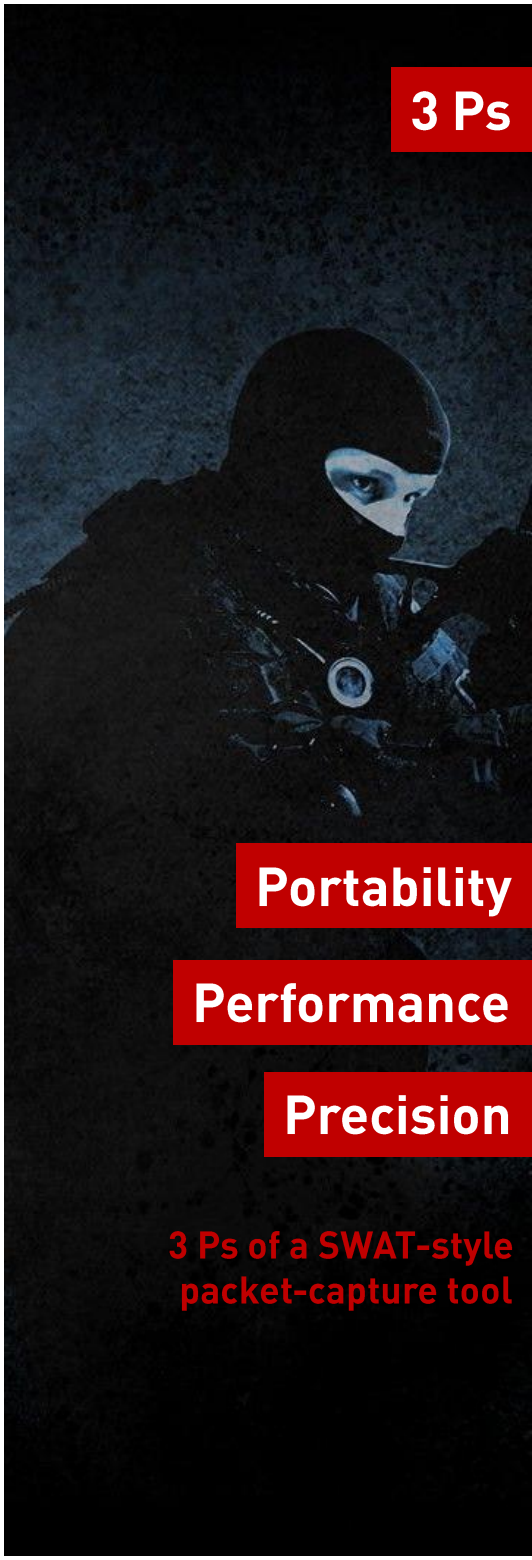
Portability

Threats in the cyberspace can originate from anywhere in the physical world. DDoS attacks, hacking attempts, network penetration, malware exploit, financial fraud – all of these events can be initiated from any location, even public places such as cafes, shopping malls, airports, or even hospitals. To counter these threats, cybersecurity units of the security forces either conduct on-ground surveillance on a periodic basis or conduct raids at suspected locations. One of the quickest ways to uncover threats occurring in real-time is to capture and analyse packets flowing over backbone network links or uplinks serving internet to WiFi access points.

A plug-&-play network TAP that could be installed instantly on network links, with the ability to scale up to Gigabit bandwidth, gets easily plugged to a laptop, is the right tool for the cybersecurity teams to quickly dive into the packets and sniff the digital conversations happening on that location. Such a tool should be portable enough to be carried around on any field location and get installed in minutes without having to configure any aspect of the active network.

Performance

In addition to being portable, this tool should be powerful enough to capture the entire traffic of interest without dropping any packets at all. Because the primary purpose of using a TAP is to have the ability to capture & analyse each and every packet. How would the cybersecurity team be able to detect an ongoing threat if it does not receive some of the packets in the first place? What if the critical packets, e.g. the ones containing the threat signature, or the defected hosts' address, or the originator's location identification, do not reach your packet analyser at all?



On top of that, analysers would not be able to reconstruct actual network flows if there are packets missing in between. So, when it comes to traffic monitoring & analysis, packet-drops simply cannot be afforded. But not all TAPs are good at capturing 100% of the packets on the wire. Specially if the network link is of Gigabit capacity since both directions of the link (east and west) aggregates to a total of 2 Gbps of output stream in full duplex mode. To remain truly portable by being usable with a laptop, the required network TAP needs to have a connection mechanism which is easily pluggable and yet does not compromise on the ability to transfer all of the packets to the laptop through a wire speed of 2 Gbps or above.

Precision

In order to counter on-ground threats while they are happening, the cybersecurity team needs to react instantly in line with the attack as it happens. For this, they need to see the data flowing over the network in real-time. Being able to capture and correlate the packets in real-time as it happens on the network is the key to ensure timely detection and suppression of cyber attacks. So even if a network TAP captures all of the packets, it also needs to ensure that the packets contain the accurate timestamp and gets delivered timely for analysis. The difference between getting busted with a cyber crime versus neutralising the attack in the first place is being able to detect & identify threats as it happens in real-time. Hence, the network TAP needs to have at least nanosecond precision built into its hardware to ensure the packets contain the actual time of its occurrence over the network.

Special tool for special forces

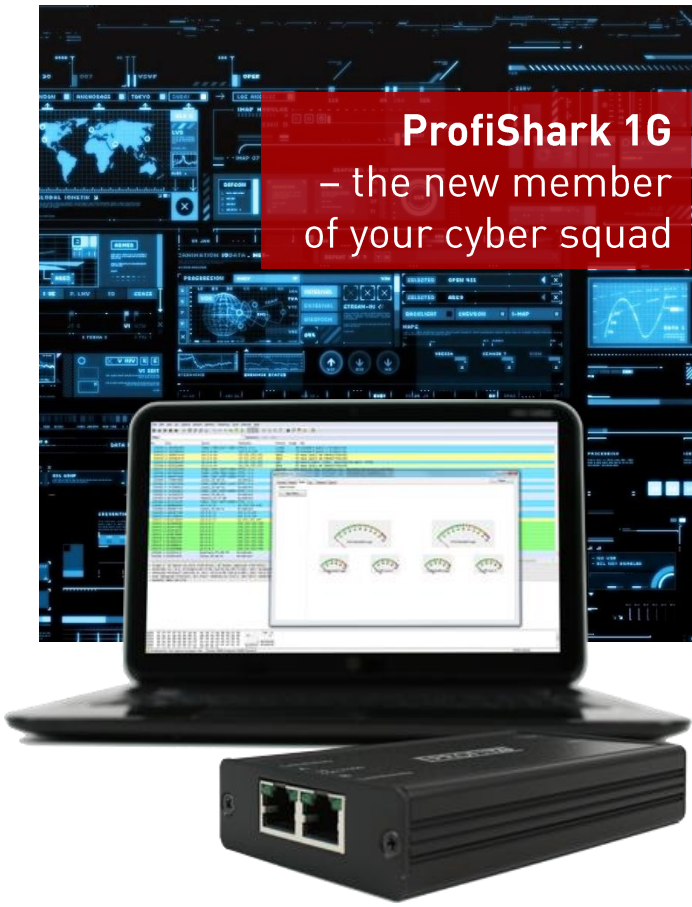
In comes the world's best, fastest and truly portable network TAP ready to hit the ground running for any kind of packet capture in any field location. ProfiShark 1G is pocket-sized and yet power-packed. It works as an all-in-one packet capture tool without the bottleneck of any packet drop or time delay. With the 2 x Gigabit network ports, it easily combines the two traffic streams to transport over a single monitoring port.

ProfiShark 1G

The ProfiShark 1G does not use a Gigabit NIC as the monitoring port. Instead, it utilises the power of USB 3.0. USB 3.0 is the third major revision of the Universal Serial Bus standard that uses a new transfer mode, SuperSpeed, which can transfer data at up to 5 Gbps. Hence it can easily transport 2 Gbps of aggregated traffic stream (1G from each direction) over a USB 3.0 link. This means that the buffer memory doesn't need to drop any packets and doesn't have to store packets long enough to impact its timing.

Because it can easily connect to your laptop's USB port, the best part of the plug-&-play ProfiShark 1G is that it is not dependent on an external power source. Combined with a laptop, you have a truly portable and powerful packet capture & analysis kit ready to use at any location without depending on a power source.

The ProfiShark 1G captures packets and transfers directly to any host computer's disk. All packets are captured in real-time with nanosecond time-stamping at hardware level on each packet as it enters the TAP. This allows real-time analysis of captured traffic with nanosecond resolution. Plus, it has the ability to capture any type of frame, be it VLAN, VXLAN, MPLS, etc., between 10 bytes and 10 Kilobytes. It also captures low level error frames, e.g. CRC errors, which makes it a perfect tool to perform troubleshooting at the lowest level as well. On top of that, ProfiShark 1G is PoE (Power over Ether-net) compliant as well, allowing the network links to transport power to the network equipments without any hindrance.



Thus cybersecurity or cyber-response teams within the law enforcement agencies or the special forces can use this special tool for any kind of on-field analysis during raids at suspected locations or during their routine periodic inspections. ProfiShark 1G is the new member of your cyber squad.

If you are interested in trying out this SWAT-style tool in field, then please contact us or visit our website for further details.

ABOUT PROFITAP

PROFITAP develops and manufactures high-quality fiber-optic & copper TAPs and Ethernet field testers to provide a wide range of hardware solutions for network analysis & traffic acquisition. With products such as the Interop award-winning ProfiShark 1G, we've fused high-performance with portability to answer the needs of countless professionals.

PROFITAP was founded in 1984 in Strasbourg, France. To this day our products are designed and manufactured in Strasbourg, where we proudly provide the same excellence that first established our brand over 30 years ago. With nearly 1,000 clients from over 55 countries, our company has become an integral solution for companies on the Fortune Global 500 list.

PROFITAP HQ B.V.
High Tech Campus 9
5656 AE Eindhoven
The Netherlands
sales@profitap.com
www.profitap.com