PHYSICAL AND CYBER SECURITY FOR UNDERSEA CABLES IN AN OPEN CABLE ENVIRONMENT

Shreya Gautam, Ronald Rapp, Richard Kram, Jonathan Liss (SubCom), Richard Pierce (Google)
Email: sgautam@subcom.com

SubCom LLC, 250 Industrial Way West, Eatontown, NJ 07724

Abstract: As the Submarine Optical Transmission Cable business continues to move in the direction of a vendor-neutral Open Cable model, increasing importance is being placed on Software Defined Network (SDN) based management. These networks include the coordination of dry plant equipment from various and sometimes multiple vendors, as well as capacity sharing across multiple owners. In addition, smart wet plant network elements such as Reconfigurable Optical Add Drop Multiplexers (ROADMs) and other common equipment such as Power Feed Equipment (PFEs) and monitoring systems create risk in terms of owner's access and interference. In addition, network owners are employing Operations Support Systems (OSS), including service orchestration that may expose networks to security risks. These new technologies and OSS implementations create new challenges for ensuring Submarine Cable System (SCS) cyber security. These new challenges add to longstanding concerns about the physical security of cable wet and dry plants. Additionally, there are concerns about cable protection methods that rely on publishing and charting cable positions to avoid accidental cuts by ship anchors and fishing gear and the risk that this information could be used for malicious intent. This paper highlights considerations and security concerns that should be addressed in Open Cable enterprises and for cable protection programs. It also offers recommendations based on the history of cable faults and technological characteristics of the element hardware and software.

1. INTRODUCTION

Deployment of Submarine Cable Systems (SCS) facilitates global data-sharing and voice communications, but it can also expose sensitive data to security threats. These critical technologies must be protected against not only physical vulnerabilities, but cyber-attacks. [1,2,3,4,5,6,7] The move to an Open Cable model creates more opportunities for threats. These challenges are not new or surprising. This paper discusses security concerns and the associated considerations.

2. MULTIPLE VENDOR EQUIPMENT

An open cable project may include separate suppliers for wet plant, dry plant, and Network Management Systems (NMS) including Operations Support Systems (OSS), Network Operations Center (NOC) services and Data Communications Networks (DCN). Additionally, phased deployments and upgrades post-system turn up suggest that there may be unforeseen challenges at the outset of a project. It is recommended that supply contracts clearly specify requirements based on industry standards for these individual systems, as well as sufficient detail to ensure reliable and seamless integration and futureproofing. Identification of a centralized maintenance authority and its responsibilities for the management of shared and dedicated equipment/services is also beneficial prior to contract adjudication. When feasible, an appropriate integration "test" phase of these systems should be allocated in project plans in addition to detailed test plans and venues.

Figure 1 provides an overview of topics discussed in this paper.

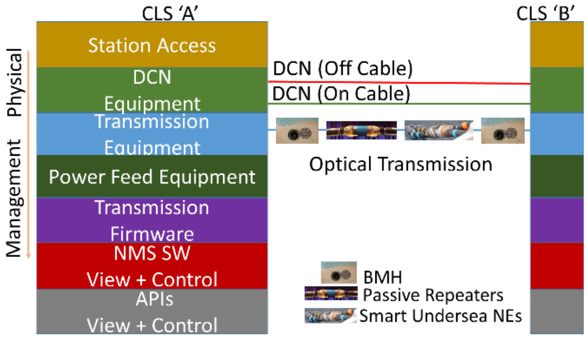

Figure 1: Overview of Security Considerations

3. MULTIPLE OWNERS OF A CABLE SYSTEM

Consortia and other types of multiple party owned SCS have joint and individual security considerations. All owners of the SCS should work together to ensure that they and their customers are fully protected from physical and cyber-attacks.

In a consortium, where joint ownership exists from day one, the landing party is typically responsible for executing the security plan within territorial waters. However, it is the responsibility of all parties to contribute to and agree upon the plan. Regular surveys or reviews of the plan should be encouraged, and the results should be shared with partners, allowing all parties to make informed business decisions and to prepare recovery plans.

In other types of ownership, the responsibilities become more complicated. These arrangements are generally completed after the ready-for-service date, so the new owners should be given an opportunity to review existing security plans and to make suggestions for changes.

4. NETWORK MANAGEMENT

Network management includes many layers of Software (SW), Firmware (FW) and DCN, inherently creating opportunities for security risks. While these systems typically do not observe or interrogate customer traffic payloads, their operation can affect data transmission. Dry and wet plant Network Elements (NE) include FW for monitoring and control and various layers of SW, including OSS, which also provides monitoring and control capabilities. If mismanaged, NEs such as the Power Feed Equipment (PFE) and smart wet plant equipment such as a Reconfigurable Optical Add Drop Multiplexer (ROADM), can cause customer traffic disruptions. These SW/FW systems are connected locally with DCN Local Area Network (LAN) equipment as well as globally with DCN Wide Area Network (WAN) equipment and services providing local and remote management capabilities and remote interfaces. DCN facilities for the latter, whether they are IP tunnels, dedicated E1 channels or satellite communications call for techniques such as encryption, password protection, certificates, etc. These remote interfaces may be hosting a Remote Operator Position (ROP) or a Software Defined Network (SDN) Machine to Machine (M2M) interface relying on Representational State Transfer (ReST). Remote and local access should include layers of client authentication, especially for operations that can reconfigure or provision equipment/services. Common network management systems require partitioning that should exist at all levels of the network management hierarchy to ensure that clients can only manage or "see" their own equipment. Open cable projects may include customers that share the cable but own individual fiber pairs, or spectrum sharing solutions.

In addition, the network management layers should be audited and provisioned accordingly for port usage and the removal of insecure low-level entry points, such as telnet and ftp protocols, to ensure that there are no open vulnerabilities.

Local or internal aggression may be the result of disenfranchised employees who may openly cause disruptions or "plant" trojans or other SW bombs. These disruptions can be best prevented by local governance, such as password cycling, user login/action monitoring and physical access control. Remote aggression may be more difficult to manage since physical environments can change without the knowledge of administrators. In addition, forensic activities maybe more difficult to detect compared to local aggression. Thus, extra care must be given to the remote facilities' user definitions and password/access management. While SDN networks provide automated and quick provisioning, they also create an enhanced possibility of network penetration. These systems must be architected appropriately to include active security. Artificial Intelligence (AI), as well as well-established security monitoring tools such as Nessus, may play a role in predicting aggressive infractions.

5. CYBER SECURITY

Submarine Cable System cyber threats can be split into two categories: data and system. Each utilize the same methodology, but they have different targets, intentions and probabilities. Data attacks include any attempt to steal payload data for the purposes of espionage, ransom or blackmail by targeting terminals, repeaters, splice points, etc. System attacks include any attempt to take over part or all of an SCS for the purpose of terrorism, ransom or vandalism by targeting the NMS, DCN, etc.

The payload data on an SCS is usually heavily encrypted, enormous and unfocused. If an attacker successfully captures data from an SCS, they must decrypt the terabytes of data and sift through it in hopes of finding specific information that they can use against an individual or organization. Their chance of success is small when compared to attacks on other portions of the network.

Cyber-attacks on the system are more likely to be successful than attacks on the data because they target the SCS components to disrupt payload. However, the probability of these attacks is low since those with the know-how to carry them out are heavily dependent on these communications channels. It is relatively easy for an SCS owner to recover from an attack of this sort, as traffic can be diverted while damaged systems are re-enabled. Therefore, successful system attacks would require significant coordination across multiple SCSs.

Although cyber-attacks on SCSs are low-risk and in many cases are easy to recover from, the results can severely disrupt isolated countries and can negatively impact the reputations of the owners. In some cases, improperly protecting against cyber-attacks could violate laws. Therefore, SCS owners must plan and budget for proper cyber protections, processes and policies and, when possible, must utilize diversity with balanced capacity and SDN.

The following are just a few basic considerations to ensure that the SCS is protected from cyber threats:

- Keep the DCN IP addresses private;
- Implement policies and processes to keep Operations, Administration, and Maintenance (OAM) computers safe through updated operating systems, anti-virus software, and Boot Input Output System (BIO0S);
- Install only OAM related software and restrict internet connections;
- Restrict admin access to essential personnel;
- Regularly change passwords and implement password complexity policies.

In addition, physical means to prevent access to sensitive equipment should be considered.

6. PHYSICAL SECURITY

6.1 Physical Security and Vulnerabilities

The risk profile to date heavily favors accidental cable cuts versus intentional or malicious acts and disruption. Approximately 90% of the 150 to 200 annual submarine cable faults are due to natural or accidental causes [8]. This section discusses faults caused by malicious or intentional actions that can be categorized as cyber-attacks, vandalism, theft (piracy), terrorism and state sponsored actions.

The network is divided into the following elements to assess its vulnerability:

- Cable station and equipment,
- Outside plant (cable station to beach),
- Inshore from beach to 20m water depth,
- Nearshore from 20m to the end of the continental shelf
- Deep sea.

Risk/ Element	Cable Station	Outside Plant	Inshore	Nearshore	Deepsea
Cyber Attack	Low	Low	Low	Low	Low
Vandalism	Mod	High	Low	Low	Low
Theft	Mod	High	Mod	Low	Low
Terrorism	High	High	High	Mod	Low
State Sponsored	High	High	Mod	Mod	Mod

Table 1: - Vulnerabilities/Impacts due to International Actions

See ref [1]. Note: Authors revised table for purposes of this paper.

6.2 Element Resiliency

Most networks are redundant and physically diverse and can sustain single or multiple breaks. Of course, this may not be true for remote landings and islands with a single cable.

Cable cuts trigger alarms at the NOC and cable station and can be quickly detected and localized, leading to the rapid dispatching of repair teams. Marine operations in the nearshore and deep-sea regions require specialized vessels and navigation equipment. Logistics and expenses help to deter criminals or other organizations from targeting offshore cables. Along the Continental Shelf, cables are typically buried, making them more difficult to locate even with precise GPS locators. Sea based attacks require more expertise and are more expensive. Therefore, terrestrial routes and cable stations are considered more vulnerable than offshore cables. However, this is typically where data and access are restricted. Other means of protection address both physical and cyber security.

6.3 Beach and Terrestrial Physical Vulnerabilities and Mitigation

The physical components most vulnerable are the Beach Manhole (BMH), the Cable Landing Station (CLS), as well as any access points between the BMH and the CLS. Land based physical attacks do not require significant expertise to execute and in most cases are relatively inexpensive to accomplish. BMHs and other access points (manhole, hand holes, etc.) are particularly vulnerable. They are typically unmonitored and, when secured, are done so with methods that may be easy to circumvent. Attacks on these points are not necessarily committed with the intent to damage the SCS, but may simply be the result of opportunities for thieves and vandals. Insufficient securing of these points can also pose a public safety hazard since they carry high voltage power cables but are not marked as such.

CLSs are less exposed than access points. Basic security measures can deter thieves and vandals who could do damage but would not impact the SCS.

The following are some physical security considerations:

- Properly secure outside plant access points,
- Ensure the CLS is fenced in where permitted,
- Use CCTV systems to actively monitor the CLS and immediate surroundings (if permitted by local laws),
- Implement policies to screen CLS personnel in accordance with local laws,
- Regularly patrol the OSP from the shore to the CLS.

6.4 Balancing Cable Protection and Cable Security

Ensuring that maritime operators are aware of the locations of submarine cables continues to be one of the primary means of protecting them from accidental damage and breaks. The cable industry has developed various means for providing cable information to marine operators [9]. As previously stated, the overwhelming majority of cable faults are due to accidental cuts, not intentional or malicious damage.

Despite these statistics, we continue to debate the questions, "Should the industry continue to promulgate cable position information (as is current practice) in light of real or perceived threats of intentional damage, network disruption, theft, terrorism, sabotage? How should the industry balance cable protection (cable awareness) with protecting cables from bad actors so that we enhance cable security?" [10]

Cable route positions and telecom cable locations are now available from a variety of sources. These include UK Hydrographic Office (HO) British Admiralty Charts, National Oceanic and Atmospheric Administration (NOAA) Charts in the US, Electronic Navigation Charts, Notice to Mariners (N-T-M) of marine operations cable laying, charts from the Oregon Fisherman's Cable Committee (OFCC) and the South Bay Cable Fishing Liaison Committee (SBCFLC), ocean planning data portals such as the Mid Atlantic Regional Council on the Oceans (MARCO), navigation apps and Automatic Information System (AIS) data sites.

In addition, cable awareness flyers are distributed to vessel operators and fishing fleets. Signage on beach manholes and CLSs identifies the location of submarine cables.

The industry practice is to protect more critical details about an SCS by withholding geographic locations that are more easily accessed or vulnerable like the beach or the cable stations. The current practice is to distribute "Agency RPLS" that show only cable positions. Repeaters, splices and other information is not provided in order to protect the proprietary nature of the data. Generally, deep sea sections of the routes away from anchoring and fishing risk are not distributed. However, recent deep seabed mining may change this. For some SCSs, precise positions on the approach to the beach and the beach manhole locations are kept private. Cable stations are not marked and are made non-descript. Company security procedures restrict access. Security initiatives include locking the BMH and handholes on an OSP route. Cable awareness programs target vessel operators and fishing fleets and cooperatives, rather than focusing on broad distribution to unknown organizations or people.

Fishermen and vessel operators need to know the locations of cables for their own safety. These are charted as hazards to navigation for all mariners. Planners of new SCSs, pipelines, umbilical's and scientific researchers or surveyors must know where to avoid existing cable infrastructure.

Uncharted cables make it nearly impossible to collect damages from a cable cut.

7. CONCLUSION

There are many other types of security vulnerabilities introduced with an open cable paradigm because of the integration of multi-vendor products and services. Vendors must follow appropriate practices during the design and manufacture phases, as well as ensure operators follow best current practices with respect to local security policies and employee vetting. When customers choose to deploy OSS for service orchestration, a new level of vulnerability is introduced, as single operations for a single seat can provide opportunities for accidental and intentional (e.g. terrorist) disruptions. Customers and owners can mitigate cyber security threats by formalizing an audit process that might include professional consultation to ensure that best current practices and government/industry standards and recommendations are being considered. The audit could include review of the integrated products, services and MOPs.

Current practices of providing cable only positions should continue in the nearshore and offshore. Distribution of materials is based on risk assessment and information is provided to known and legitimate fishing fleets and vessel operators to the extent possible. Security has more impact if focused on more easily accessed areas of the terrestrial route and cable station versus the submarine portion. It is recognized that the consequence of multiple intentional cuts may be greater than a single or a few accidental cuts.

Open cable projects offer owners flexibility in design, vendor independence and futureproofing. These freedoms inherently create challenges related to ensuring physical and management security. This paper introduced topics for consideration when planning such projects.

8. REFERENCES

[1] Dean, J. et al., ‘Threats to Undersea Cable Communications,’ The Public-Private Analytic Exchange Program (AEP), sponsored by the Department of Homeland Security’s Office of Intelligence and Analysis (DHS/I&A), September 28, 2017.

[2] Runfola, J.A. ‘Undersea Cables: A Defense Vulnerability, Sea Technology, p49, Nov 2018.

[3] Davenport, T., ‘Submarine Cables, Cybersecurity and International Law: An Intersectional Analysis’, Catholic University Journal of Law and Technology, Volume 24, Issue 1, Article 4, P.82, Dec 2015.

[4] BBC, ‘Russia a 'risk' to undersea cables, defence chief warns’, 15 Dec, 2017. https://www.bbc.com/news/uk-42362500

[5] Bardelay-Guyot, C , Barezzani M., “ Network Management Systems
How to Improve System Security”, SubOptic 2013.

[6] Bressie, K. “Coping Effectively with National-Security Regulation Of Undersea Cables,” SubOptic 2013.

[7] Patel, M., ‘Network Security for Submarine Networks’, SubOptic 2013.

[8] Kordahi, M.E, et al. ‘Global Trends in Submarine Cable System Faults’, SubOptic 2016.

[9] International Cable Protection Committee, Recommendation 5 & 6. https://www.iscpc.org/

[10] Rapp, R., ‘Balancing Cable Protection with Cable Security’, ICPC Plenary Meeting, Cape Town, South Africa, April 2018.