NETWORK MANAGEMENT SYSTEMS HOW TO IMPROVE SYSTEM SECURITY

Caroline Bardelay-Guyot , Michele Barezzani (Alcatel-Lucent Submarine Network)
Email: caroline.bardelay@alcatel-lucent.com

Alcatel-Lucent Submarine Networks - Centre de Villarceaux, Route de Villejust – 91620 Nozay, France

Abstract:
Security of the submarine network management is a complex subject requiring everybody's commitment. In this article, we present two axes of intervention that are usually followed to improve the network management security, logical security and physical security, together with secured network sharing. In addition, we suggest how to implement simple security practices in submarine networks and describe certain situations that may weaken the overall network security.

1. INTRODUCTION

Network management systems constitute a privileged access point to the submarine network.
They allow to monitor and control terrestrial & submerged equipment (Terminal, Power Feeding Equipment (PFE), Repeater, Branching Unit) as well as network overall status usually including fault detection. Network management systems also provide provisioning, monitoring and analysis of optical channels and end-to-end services and performance control.
Such information systems are therefore a critical element of the submarine network: their availability, reliability and overall security are essential to ensure uninterrupted operations and to optimize the Return On Investment (ROI) of the network.
The purpose of this paper is to analyze these security needs and to propose possible solutions to improve the security of network management systems.
Security of the submarine network management is a complex subject requiring everybody's commitment.

"Qui non est hodie, cras minus aptus erit"
"He who is not prepared today
will be less so tomorrow"
Ovid, Roman poet

2. ABOUT SECURITY

Security and Safety

Cyber Security is a set of concepts, techniques and procedures intended to protect systems and networks from unauthorized activities or untrustworthy individuals (hackers) and unplanned events.
Cyber Security is therefore different from Safety (electrical, optical, mechanical, thermal, fire, operations), although both contribute to the availability of a system.
Facing growing needs of new opened services, Cyber Security is a growing concern for all manufacturers and network owners.

Cyber Security

Cyber Security deals with the eight security dimensions of end-to-end communications (cf. ITU-T X.805).

Access control protects against unauthorized access to network resources.

Authentication serves to confirm the identity of communicating entities (person, device, application or service).

Non-repudiation prevents an individual or entity from denying having performed a particular action: it provides evidence that can be presented to a 3rd party as a proof.

Data confidentiality ensures that data content cannot be understood by unauthorized entities (file permissions and encryption are typical methods used to ensure data confidentiality).

Communications security ensures that information flows only between the authorized endpoints and is neither diverted nor intercepted.

Data integrity protects data against unauthorized modifications, deletion, creation, and replication, and provides an indication of these unauthorized activities.

Availability ensures that there is no denial of authorized access to NE, network resources, services and applications.

Privacy ensures that information cannot be derived from the observation of network activities (e.g. visited web-sites, user's geographic location, time spent on a network resource etc.).

3. TYPICAL SECURITY THREATS IN SUBMARINE NETWORKS

Here are examples of the key threats facing submarine networks:

- Destruction of information and/or other resources: e.g. traffic matrix, NE configuration tables, system files, software applications,
- Corruption or modification of information: e.g. as above or performance data files, log files and in particular security log files,
- Theft, removal or loss of information and/or other resources: e.g. traffic eavesdropping, credentials, passwords, software applications,
- Disclosure of information: e.g. alarms, performance data or other sensitive information,
- Interruption of services: e.g. transmission, powering, supervision, management, DCN, inter-station communications,
- Impairment: e.g. management services slow-down, DCN through-put reduction,
- Misuse: e.g. surfing on Internet with station PC, using station systems for personal tasks,
- Exfiltration, data leakage: e.g. unauthorized copy of system data via removable media (e.g. USB keys).

4. WHAT TO DO?

Products and networks shall be built "with security in mind" at each step of their design.

Owners of networks should have Security Policies and should have them actively in place (cf. ISO 27000).

The security policy allows making stations and NOC personnel sensitive to any security aspects in the day-to-day activities.

Although improving the security of a network requires an in-depth case-by-case study, it is possible to highlight at least two general axes of intervention that will always be followed:

- Logical security
- Physical security

LOGICAL SECURITY

Improving the logical network security requires working on several aspects, like:

- Hardening
- Firewalls
- Antivirus
- Data encryption
- Communications encryption
- Security patches
- Authentication

Hardening

Hardening is the process of securing a system by reducing its surface of vulnerability (cf. [3]).

The vulnerability surface increases with system complexity. Hardening is intended to make attacks more difficult by reducing, removing, or fixing vulnerabilities by turning off unused services, as well as minimizing the number of used ones. Hardening a computer may require several defense mechanisms to form multiple layers of protection, each of which present unique obstacles to the adversary. This approach to safer computing is often called "defense in depth": its main objective is to delay and make the attacks more and more complex.

Hardening includes the removal of unnecessary software, unnecessary usernames or logins, closing open network ports, and setting up intrusion-detection systems, firewalls and intrusion-prevention systems.

Firewalls

A firewall prevents unauthorized external connections from entering the system.

In addition firewalls provide a useful protection against network-level attack (e.g. Denial of Service attacks, Pin-of-Death attacks).

Firewalls must be used to protect network management systems.

However a firewall is not an antivirus. It does not identify or remove any virus or worms carried within authorized programs.

Antivirus

Antivirus software tools are used to prevent, detect and remove viruses, i.e. a computer program that can replicate itself and spread from one computer to another. New viruses are created every day, so that the efficiency of an anti-virus is directly related to its capability to be updated with the most recent countermeasures.

Updating an antivirus software tools requires connecting to an external server. This connection must be carefully secured, unless it would become itself a potential security issue.

Data encryption

Sensitive data stored by the network management system must be encrypted so that they become unusable by unauthorized persons.

Examples of data potentially requiring encryption include user access rights and security logs. Submarine network configuration and monitoring information such as events and performance data may also require this kind of protection.

Communication encryption

The hardened network management server communicates with other elements of the network management plan:

- with the Submarine Line Terminal and the Power feeding equipment to get information and to send commands,
- with the OP/ROP PCs to interact with operators to display information and get requests,
- with other network management servers, for example in case of geographical resilience.

The encryption of those communications is necessary to reduce the risk of interception and misuse (e.g. man-in-the-middle attacks, password and sensitive credential sniffing).

SSL/TLS is commonly used to encrypt communications between two software entities. SSL is a set of protocols that provides privacy, authentication and reliability between two communicating applications. It is therefore recommended to use protocols that support encryption, https and ftps.

SSH (Secure Shell) is a suite of programs that allows remote users (especially system administrators with Command Line Interfaces) to securely access systems. SSH provides encryption and stronger authentication than protocols such as telnet and ftp. SSH is highly recommended for remote system administration.

Security patch management

Security vulnerabilities can be discovered on network management systems, especially on used Operating Systems (OS) and third party products (3PP).
System providers should have an organizational process in place to enable timely handling of new vulnerabilities discovered in the software platform. Appropriate corrections for the system are delivered as security software patches.
On the other hand, at product design time a careful choice of OS and 3PP can help to minimize the need of security patches.

Authentication

Appropriate mechanisms need to be implemented for strong authentication of the operators and, based on their role, assign corresponding levels of access rights.

Network management system access to the network elements must also be authenticated.

A strong password policy shall be implemented on network management system e.g.

- impose a minimal password length (12 characters or more),
- passwords must be case sensitive, including numerical and special characters to deter brute-force attacks,
- change password on a periodic basis, ensuring that the new password is different from N previous ones,
- use complex combinations of characters, excluding dictionary terms and names,
- adopt a secure password distribution protocol,
- avoid sharing a same password between more users or for more systems,
- perform password audit on regular basis.

Some other authentication devices may also be used such as USB token, smart cards, and even biometrics.

PHYSICAL SECURITY

Physical security is not limited to station access control, doors and locks: it encompasses various human and organizational aspects.

Human aspects

All personnel having access to the submarine station or the NOC should be informed about cyber-security. The need is to reduce risk of misuse of secured system.
Here are some human aspects of the security policy that concern network management system usage.

Authentication system should be used to control all access to stations or NOC rooms.

Authentication credentials are personal and cannot be shared among the personnel, or displayed to anybody.

Connections to internet should be controlled. Internet should only be accessed from well identified and secured PCs, disconnected from the submarine network.

Malicious intent

Attacks from inside the organization are extremely dangerous, but they are difficult to perpetrate and often visible enough to become unlikely: the role of security logs in discouraging this kind of intentions is fundamental.
In any case, the personnel of stations and NOC should be motivated to protect the company's assets (equipment, software, and data).
Departure of a person should be properly managed (get badge back, delete accounts and change all passwords).
System security is fragile and relies on continuous attention to details.

5. SECURED NETWORK SHARING

System Security also concerns user access rights and particularly secured sharing administration of network resources between users.
Network management system should offer full flexibility in user access rights management to make carriers O&M activities optimized.

People in stations and in NOCs need to have different access rights depending on their roles and on their ownership in the network.
Operators should only be granted the minimum level of rights requested by their role: a particular attention should be paid in using and distributing the Administrator rights.

Why resource sharing?

Many submarine networks are owned by consortia. The topology and capacity of the network is often shared between carriers. At network management level, the sharing of those network resources can be needed. Data confidentiality may require hiding the management of some parts of the network to some users. For example, performance data of a fiber pair may be critical competitive information that should be

accessible only to some users and not others.
Resource sharing can be simplified with the introduction of the concepts of access domain and functional domain.

An access domain is the set of resources (typically segments, fiber pairs, SLTE, PFE, BU, trunk line, branch line…) to which an operator is granted access.
Here are some examples:
A user in a trunk station can have access on the segment its station is connected to and not other segments of the network.
A user in a branch station can have access on the branch line part of the network and not the trunk line part.

The functional domains can be seen at two levels.
Each user has an affected role, also called profile, in the organization. Typically, network management applications provide three predefined roles: observer, operator and administrator. Other specific roles like security administrator can be defined.
Some dedicated functions are affected to each role. Network management application makes the management functions available to the user depending on that affected role.
The functional domains may need to be adjusted to offer full management flexibility. Some users may need to monitor some resources and at the same time to control some other resources.
Here are some examples:
A user in a station with administrator role may be authorized to control the SLTE in its station but only observe the SLTE in the distant station.
A user in a branch station with administrator role may be authorized to control the BU facing its branch but only observe the other BU of the segment. And even more this BU control can be only on electrical configuration capability of the BU and not on the optical configuration capability of the BU.

Secured administration

The user access rights have to be managed, and managed in a secure manner.
Only selected and well defined users must be authorized to define and change the user access rights. Those users should have a special super-user authentication.
The user access rights information have to be securely stored to not be easily changed or made unusable by unauthorized persons.

6. WHAT NOT TO DO

Submarine network management systems are very often installed in a closed private Data Communication Network (DCN), disconnected from all other networks. This isolation is a very positive security advantage, but unfortunately it is not easy to conserve in the medium/long term as it will be shown in this section.

Most current security risks

Let’s consider a few examples of events occurring in everyday life of submarine network management systems and potentially affecting their security, mainly by disclosing the DCN or the management system to potential attacks.

A first example concerns the usage of USB keys: it is well known (e.g. Stuxnet virus), that spectacular cyber attacks to highly protected sites have successfully been realized by the simple introduction of an infected USB key in the system. In submarine networks, operators have often the need to transfer performance data and export data files, and an USB key is an ideal media for that. But USB key can be infected with various worms and Trojan horses so that their usage has to be subject to a strict security control.
That is why certain equipment suppliers request to use only brand new or virus-free USB keys for data transfer and discourage the connection of the station equipment (e.g. the PC of the operator position) to any USB devices (e.g. cameras)
Of course this recommendation is not sufficient yet and requires a strict discipline.

A second example of threat to the submarine network security: network operators may be tempted to connect unused ports of the DCN routers to other devices and even to other networks, in an attempt to optimize or reduce costs or for practical reasons. This may well open the back door to potential malicious attacks.

More and more network operators control their networks from remote sites: operations are no longer confined within submarine stations and NOCs. This imposes serious security controls on both the PC used for the connection and the remote connection itself: inadequate or low level security will be clearly a security threat to the submarine network.

It is also noticed that alien software is sometimes installed on station or ROP computers by network operators or station personnel: those added software parts may not come from a secure source and again may be bearers of bugs, worms and all other sort of cyber threats. Moreover, they are not part of the supplied System. Some unforeseeable side effect events may happen during or after such installation, a further risk for the system availability.

Eventually, ROP computers have not to be used for other purpose like office work or, even worse, home or personal activities.

This set of examples is certainly incomplete, but it should be clear that each of these situations put at risk the integrity and/or the availability of any submarine network system.

However, although a zero security risk position cannot be achieved, we should be reassured by the fact that the application of a few basic security principles in a disciplined and permanent way will very much improve the resistance of submarine networks to cyber attacks.

7. CONCLUSION

Submarine network management systems have generally a good level of logical security until the DCN remains a closed environment. No breaches mean low risks.
We have mentioned in this paper several examples of basic security risks, suggesting simple precautions to adopt to

improve the network strength or to reduce its surface of vulnerability.

The overall security level of a network is determined by the lowest security level of each of its components. So security must be a concern for everyone.

8. REFERENCES

[1] Standard ITU-T X.805
[2] Standard ISO 27000
[3] Hardening - CIS Benchmark documents (www.cisecurity.org)