7SHIELD

KR11 – Detectors
Combined C/P Threat Detection and Early Warning module

Modules

- Geospatial Availability Detection Monitoring (ADM)
- Radio- Frequency Interference Detection and Identification (RFIDI)

Detection

Sensors Technologies

Scope

7SHIELD platform is designed to **detect** any **cyber and physical attacks** to the Satellite Ground Segments (GS).

The **ADM** constantly monitors the availability of the Critical Infrastructure (CI), sends messages to the Availability Correlator (AC) which sends back its event to the Hyper Combined Correlator (HCC).

The radio frequencies used by the antennas of the GS to receive critical data from satellites can be a victim of interference, intentional or not. The **RFIDI** module can use the signal quality reception parameters (C/N, MER, BER) as well as other data (weather, satellite technical condition, historical data) to detect and identify such interference. Moreover, the RF events collected are filtered and correlated through correlation rules designed by means of the dedicated component of Cyber Attack Detection Framework.

The 7SHIELD platform collects the message sent by the detectors via **KAFKA broker** and issue an alarm on the Command and Control Room (ENGAGE and CPTM Dashboard).

This project has received funding from the European Union's Horizon 2020 Research and Innovation Programme under Grant Agreement No 883284

Partners

CS Novidy's
France

CS Novidy's (CSNov) is a company specialised in Cybersecurity and IT Transformation solutions and services.

EETT
Greece

Hellenic Telecommunications & Post Commission (EETT) is the national regulatory authority with the competence to manage and monitor the monitor the use of radio frequency spectrum in Greece.

CeRICT
Italy

Centro Regionale Information Communication Technology sclr (CeRICT) is a research consortium of Italian computer scientists and engineers cooperating in the Information and Communication Technology (ICT) domain.

Stakeholders

The ADM and RFIDI modules can be integrated into **any Satellite Ground Segment** to provide signal that will aid for the detection and identification of an unavailability of the CI or an RF anomaly.

All the modules developed in the frame of 7SHIELD have been designed with the consultancy of identified external stakeholders, first responders and following the **requirements** provided by the partners working in the space sector acting as Pilots, who provided the Critical Infrastructures for **testing and demonstration**.

Purpose

The 7SHIELD framework is proposing two combined C/P Threat Detection modules.

The **ADM** monitors the availability of devices, servers, services and 7SHIELD infrastructure modules and alert in case of availability status changes.

The **RFIDI** evaluates the parameters related with the quality of the reception of the Satellite data in order to detect anomalies in the communication between the Satellite and the Ground Segment, correlates other input (e.g. weather conditions, historical reception data) and extracts sound conclusions regarding the reason of the anomaly (e.g. radio frequency interference (RF)).

Contribution

CSNov is specialist for the Network Operations Center (NOC) services and Security Operations Center (SOC) services and designed and developed the ADM, based on NOC tools.

EETT's Spectrum Department is involved in the 7SHIELD project providing expertise on wireless communications, possible ways that RF interference can affect the reception of data and the procedures to detect and identify any unauthorized use of Radio Frequencies. EETT provided the rules for the implementation of the RFIDI module.

CeRICT created a correlation rule that made the Correlator (KR08) analyze data provided by the probes, and feed to the Kafka Broker according to the logic provided by EETT.

Contacts

- charlelie.morineau@csnovidys.com
- gaetan.dedobbeleer@csnovidys.com
- 7shield_eett@eett.gr

Methodology

RF communications can be affected by many parameters. These include antenna (Transmitter and Receiver) characteristics, distance of the RF link, weather conditions, transmitter power, other transmissions and obstacles near the receiver area, etc.

The RFIDI module is monitoring the reception parameters and compares them continuously with a set of parameters that can define the "normal operation".

Whenever the observed reception parameters deviate from the above, the RFIDI module raises an alert according to the predefined rules. These rules include parameters and values for historical data, information of a malfunction of the Satellite, weather conditions, etc.

The ADM tool is a customization of the Nagios core in order to perform availability checks from very simple cases to very complex ones.

.

Future Improvements

The RFIDI operation is based on a set of quality parameters extracted from the received satellite signal.

However, in the case that the GS does not monitor the quality parameters of the received satellite signal, **a specialized sensor** may be developed and installed in the Satellite GS infrastructure in order to monitor these parameters and feed the 7SHIELD platform with the related data. The proposed sensor would allow the RFIDI module to function without any operational requirement on the GS infrastructure.

www.7shield.eu