Attack Scenarios on IEC 61850 GOOSE Messages

Introduction

The IEC 61850 standard is pivotal in ensuring communication within substations, particularly through the use of GOOSE (Generic Object Oriented Substation Events) messages. GOOSE messages play a critical role in the real-time exchange of status information and control commands among Intelligent Electronic Devices (IEDs). However, their security is paramount to prevent malicious manipulation that can disrupt substation operations. This report delves into various attack scenarios tested on GOOSE messages to evaluate their vulnerabilities and system responses.

Attack Scenarios

1. Data Manipulation

Overview:
Data manipulation attacks involve altering the values of certain fields within GOOSE messages to test the robustness of the Intrusion Detection System (IDS).

1.1. Data Manipulation (DM) in `stNum` & `sqNum`

Description:
This test case involved injecting GOOSE messages with abnormally high values for the state number
`stNum` and sequence number (`sqNum`). The purpose was to evaluate the IDS's ability to detect anomalous increments that deviate significantly from the normal progression.

Execution:

- The attack script modified the GOOSE messages by setting `stNum` and `sqNum` to high values far beyond typical operational ranges.
- These modified messages were then injected into the network to observe the IDS's response.

Results:

- The IDS successfully detected the anomalous increments in `stNum` and `sqNum`.
- Logs showed clear alerts indicating abnormal values.

1.2. Data Manipulation (DM) in `stNum`, `sqNum`, and `bool`

Description:
This test case involved direct manipulation of the `stNum`, `sqNum`, and `boolean` data within the GOOSE messages. The aim was to see how well the IDS could detect a combination of multiple manipulated fields.

Execution:

- The attack script simultaneously modified `stNum`, `sqNum`, and `boolean` data in the GOOSE messages.
- These manipulated messages were injected to test the IDS's detection capability.

Results:

- The IDS flagged the manipulated fields promptly.
- Detailed analysis confirmed that the combination of changes was effectively identified.

1.3. Data Manipulation in `stNum`, `sqNum`, and `GOOSE Length`

Description:

This test case focused on manipulating `stNum`, `sqNum`, and the length of the GOOSE message. The objective was to test the IDS's ability to detect inconsistencies in multiple parameters, including the overall message length.

Execution:

- The attack script adjusted `stNum`, `sqNum`, and modified the length of the GOOSE message to create an anomalous packet.
- These packets were injected into the network to observe the IDS's response.

Results:

- The IDS successfully detected the inconsistencies across multiple parameters.
- Alerts were generated for both the state/sequence numbers and the unusual message length.

1.4. Data Manipulation in `GOOSE Length`

Description:
This test case isolated the manipulation to the length of the GOOSE message. The purpose was to see if the IDS could detect anomalies based solely on the length of the messages.

Execution:

- The attack script modified the length field of the GOOSE messages without altering any other parameters.

- The modified messages were injected to test the IDS's response to length anomalies.

Results:

- The IDS detected the abnormal length values effectively.
- The detection of length anomalies was consistent across all injected packets.

1.5. Data Manipulation in `sqNum`, `stNum`, `bool`, and `GOOSE Length`

Description:
In this test case, the focus was on manipulating all the important parameters of the GOOSE message. The goal was to evaluate the IDS's sensitivity to changes in these sequence-related parameters.

Execution:

- The attack script modified `sqNum`, `stNum`, `boolean`, and GOOSE length values in the GOOSE messages.
- These heavily manipulated messages were injected to test the IDS's comprehensive detection capabilities.

Results:

- The IDS flagged the combined manipulation of all parameters.
- Detailed logs confirmed that the IDS could handle complex, multi-field attacks effectively.

---

2. Denial of Service (DOS) Attack

Overview:
A Denial of Service (DOS) attack involves overwhelming the system with a flood of GOOSE messages to disrupt normal operations and exhaust resources.

Execution:

- The attack script generated a high volume of GOOSE messages in a short period.
- The IDS's ability to handle the flood and maintain performance was evaluated.

Results:

- The IDS successfully detected and mitigated the flood of messages.
- System performance remained stable despite the high volume of traffic.

---

3. Replay Attack

Overview:
A Replay attack involves capturing legitimate GOOSE messages and retransmitting them to the network to create confusion and potentially trigger erroneous operations.

Execution:

- Legitimate GOOSE messages were captured using a network sniffer.
- The captured messages were replayed into the network to test the IDS's ability to recognize and block these replayed messages.

Results:

- The IDS effectively identified and blocked the replayed messages.
- Logs indicated successful detection of duplicate messages.

Impact

In all test cases mentioned above, the IDS successfully detected the manipulations. This demonstrates the robustness of the IDS in identifying a wide range of anomalies in GOOSE messages, from simple field changes to complex multi-parameter manipulations and high-volume attacks.

Conclusion

The IDS algorithm demonstrated robust detection capabilities across a variety of test cases, successfully identifying all simulated attacks. The comprehensive testing, including manipulation of individual and multiple fields, confirmed the IDS's effectiveness in safeguarding the real-time system against various types of GOOSE message anomalies.

Author: Shaheem Mushtaq

Date: July, 2024