

Goose Replay Attack

Keywords: IEC 61850, GOOSE protocol, payload,

Requirements:

- (1) `$ python3 -m pip install scapy pyshark`
- (2) Goose Receiver Simulator : <https://www.infotech.pl/products>
(<http://www.infotech.pl/downloads/61850Avenue/Avenue.2.1.11.201210131109.Trial.zip>)

Run:

```
$ python3 GooseReplayAttack.py
```

Screenshots Step by Step:

GOOSE Receiver

File Transmission Data Help

Network adapter Ethernet MAC: 6C-02-1B-7F-9D-4E

Type Not routable

Ethernet

Source 50:50:51:00:00:00 Own

Destination 01:0C:CD:01:00:00 M-cast

VLAN

Priority 4

☒ VLAN header CFI Eth

ID 0 H

IP

Address 239.1.1.35 M-cast

GOOSE

App ID 1 H

TTL 0

DSRef LLN0\$DS4

CBRef LLN0\$gcb1

GID G1

Time 2021-06-01 09:17:28.513

StNum 0

SqNum 0

CfgRev 1

NComm FALSE

Test FALSE

Status No data

Data items

Idx	Type	Value	Data reference
0	BOOL	FALSE	

Option 1 : Selection of option [1], it means that send an old recorded pcap file to Goose Receiver Simulator

The screenshot shows the Goose Receiver application window and a Windows command prompt. In the Goose Receiver window, the 'GOOSE' tab is active, and the 'Status' field is highlighted in red with the text 'Old data'. The 'Data items' table is also visible.

Idx	Type	Value
0	BOOL	FALSE
1	INT	32
2	BOOL	FALSE

The command prompt shows the execution of the script `C:\Users\user\Ferdi\Desktop>python GooseReplayAttack.py`. The user is prompted to enter an interface name and then selects option [1]: send pcap frame. The script then prompts for a saved pcap file, and the user enters `goose_packet`. The output shows 'Sent 1 packets.' repeated multiple times.

Option 2 : Selection of option [2], it means that send a payload to Goose Simulator

The screenshot shows the Goose Receiver application window and a Windows command prompt. In the Goose Receiver window, the 'GOOSE' tab is active, and the 'Status' field is highlighted in red with the text 'Old data'. The 'Data items' table is also visible.

Idx	Type	Value
0	BOOL	TRUE
1	INT	10
2	QUALITY	0.1000000001

The command prompt shows the execution of the script `C:\Users\user\Ferdi\Desktop>python GooseReplayAttack.py`. The user is prompted to enter an interface name and then selects option [2]: send frame payload. The script then displays a detailed hex dump of the frame payload, including fields like `prio`, `id`, `vlan`, `type`, `load`, `dst`, and `src`. The output shows the hex dump of the frame payload.