Lab 2: Man-in-the-Middle Attacks on GOOSE Communication

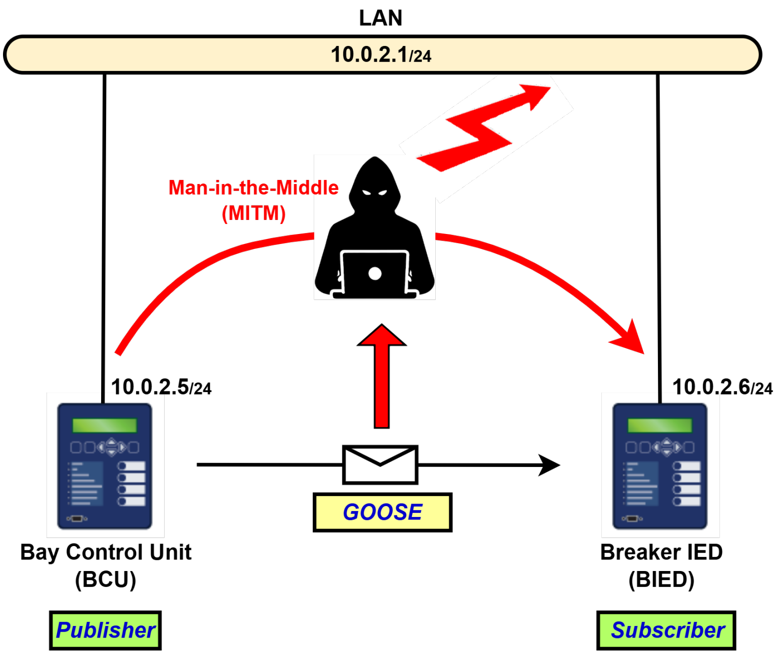

Figure 1: Conceptual illustration of a MITM replay attack on GOOSE messages

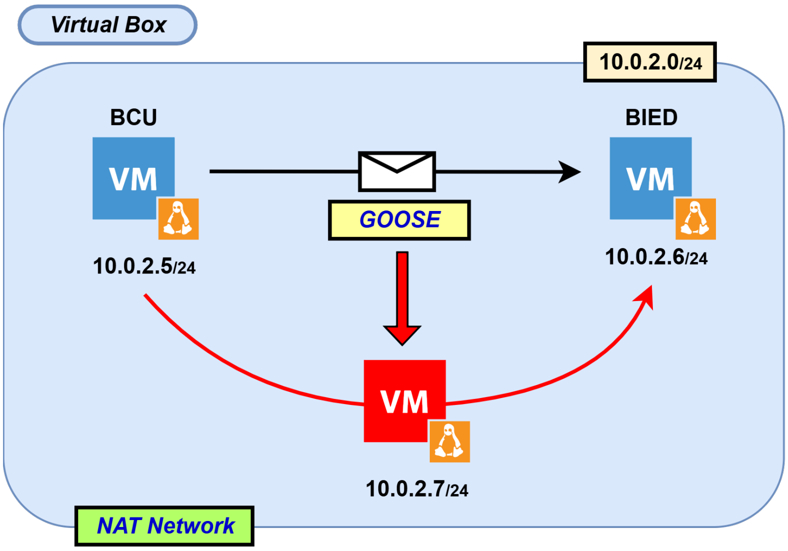

Figure 2: Practical MITM attack setup using an attacker VM in the virtualized network

Install Tools

```
sudo apt install scapy libpcap-dev tcpdump
```

- goose_capture.sh and masquerade_replay.py

```
    sudo chmod +x <file_name>
    sudo ./goose_capture.sh
```

- Establish communication between **BCU** and **BIED**.
- Press Ctrl+C on **MITM** after you capture enough packets.

Packet Modification

```
sudo python ./masquerade_replay.py enp0s3 goose_capture.pcap
   modified_goose_capture.pcap 168 02 10
```

- It will replay the packets, and **BIED** will receive them.

Lab02: (Optional) Rule based Anomaly detection

Subscriber: code snapshot

```

// Global variables to keep the last state

volatile int stNum_t1=0, sqNum_t1=0;

//Local to the sigint_handler subroutine
int stNum_t, sqNum_t,a_t=0;

    stNum_t = GooseSubscriber_getStNum(subscriber);
    sqNum_t = GooseSubscriber_getSqNum(subscriber);

    if (stNum_t1 != stNum_t && stNum_t != (stNum_t1+1))a_t =1;
    else if (stNum_t == stNum_t1 && sqNum_t != (sqNum_t1+1))a_t =1;
    else if (stNum_t == (stNum_t1+1) && sqNum_t != 0)a_t=1;
    else a_t =0;

    if(a_t ==1)
    {
        // Necessory operations i.e. GOOSE parsing
    }
```