Università del Piemonte Orientale

Dipartimento di Scienze e Innovazione Tecnologica

Corso di Laurea in Informatica

# ATTACCHI AL PROTOCOLLO MMS

Tutore interno:

Prof.ssa Lavinia Egidi

Laureando:

Andrea Ierardi

Anno Accademico: 2018/2019

# Obiettivo dello studio

- Realizzazione di **attacchi informatici** contro il protocollo MMS con supporto alla crittografia TLS
- Analisi e ricerca delle **vulnerabilità** del protocollo TLS

**Studio guidato**

Collaborazione scientifica dell'Ateneo con l'azienda Ricerca sul Sistema Energetico (RSE)

# Tecnologie utilizzate


- Container Docker
- Reti Docker


- Fasi dell'handshake TLS


- Modello a Oggetti
- Server e client MMS

# Lavoro svolto

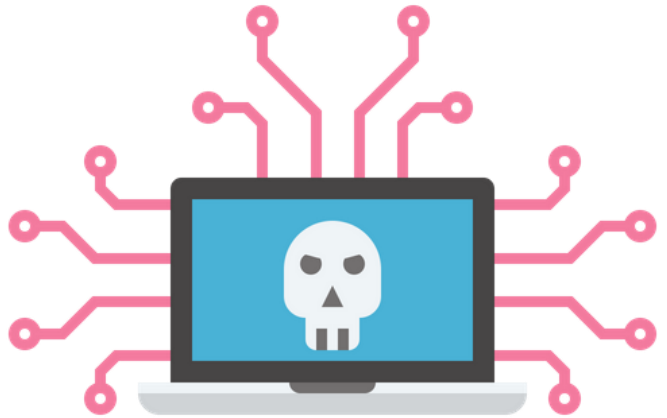
- Ricerca sulle vulnerabilità del protocollo TLS e dei cipher suite
- Ricerca di attacchi
- Ricerca e realizzazione di strumenti di attacco
- Realizzazione degli attacchi

# Vulnerabilità di TLS e dei cipher suite

| Concettuali dello standard | Primitive crittografiche deboli | Implementazione |
|---|---|---|
| ○ 3SHAKE<br>○ POODLE<br>○ LOGJAM<br>○ FREAK | ○ SWEET32<br>○ ROBOT<br>○ LUCKY13 | ○ BEAST ○ SLOTH<br>○ CRIME ○ DROWN<br>○ BREAH ○ ROCA<br>○ HEIST |

# Attacchi sviluppati

- Attacco Man in the middle passivo ✓
- Attacco Denial of Service ✓
- Attacco Packets Filtering ✓
- Attacco Downgrade ✗



# Software testati

| Man in the Middle | Denial of Service | Packets Filtering | Downgrade |
|---|---|---|---|
| ○ Arpspoof e TCPdump<br>○ Ettercap<br>○ SSLsplit | ○ Script Scapy<br>○ Websocket-bench | ○ NetfilterQueue | ○ NetfilterQueue |

# Strumenti per il Packets Filtering

**NetfilterQueue**

Libreria Python per l'alterazione e rifiuto dei pacchetti

**Arpspoof**

Software per il poisoning delle tabelle ARP

ARP SPOOFING
arpspoof

**TCPdump**

Software per l'intercettazione dei pacchetti

TCPDUMP
& LIBPCAP

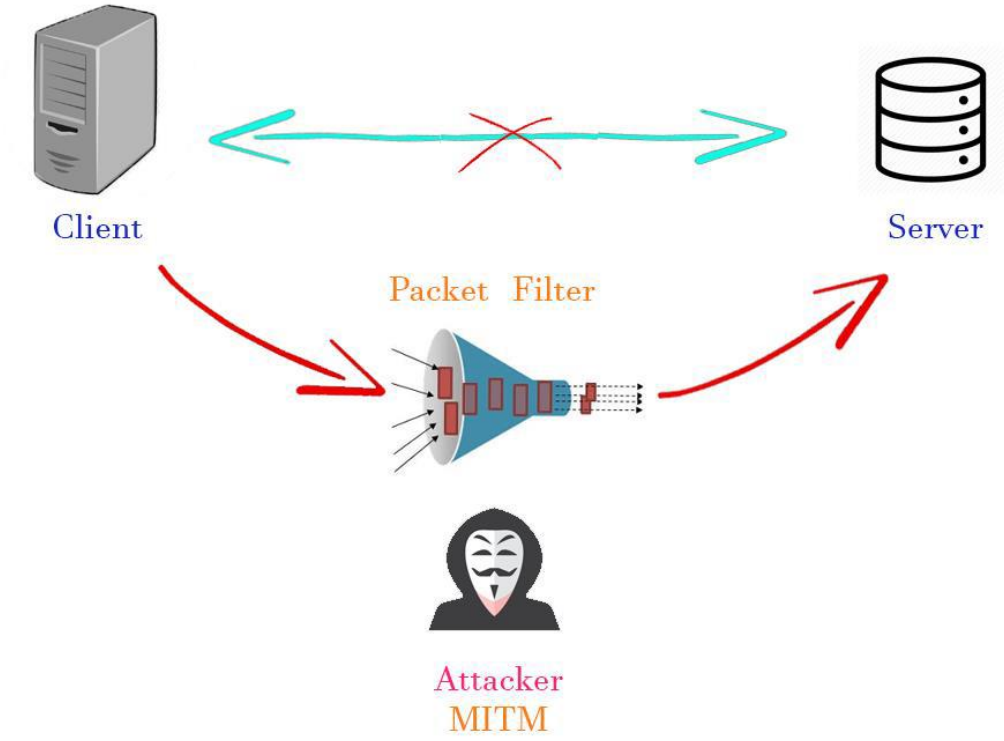
# Attacco Packets Filtering

**Implementazione del Man in the Middle**

- Alterazione delle tabelle ARP
- Intercettazione dei pacchetti

**Filtraggio dei pacchetti**

- Per dimensione
- Per numero



# Strumenti per il Denial of Service

**Scapy**

Libreria Python per la manipolazione, decodifica e forgiatura di pacchetti di rete


**Websocket-bench**

Software di testing di websocket server

# Attacco Denial of Service

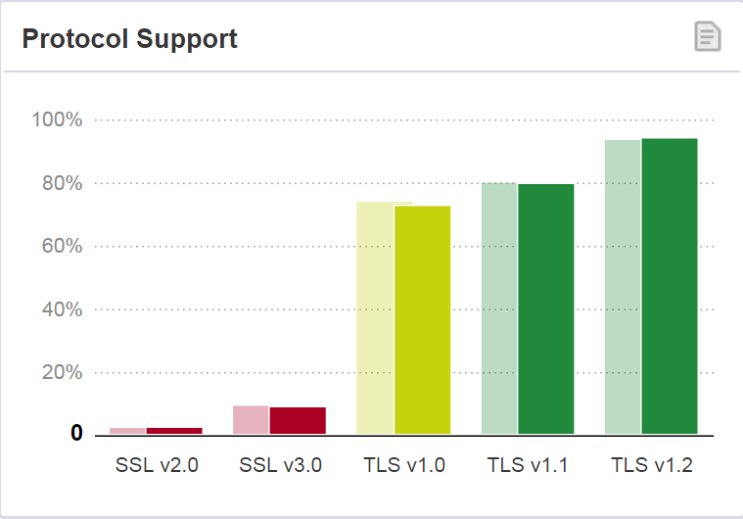
**Scapy**

Implementazione di un attacco SYN flood

**Websocket-bench**

Instaurazione di una moltitudine di connessioni con il server MMS fino a saturarne le risorse

# Conclusione




La maggior parte dei dispositivi supporta **versioni obsolete** del protocollo di cifratura TLS

**Sviluppi futuri**

- Approfondimento sull'attacco Downgrade
- Possibile riadattamento di SSLsplit per MMS
- Aggiunta della decifratura per il MITM

**Nessun dispositivo è perfettamente sicuro!**

# Grazie per l'attenzione!