

# Aspects of high speed network monitoring

Yacine Bouzida  
Bouzida@tcl.ite.mee.com

## IEEE/IST Workshop on "Monitoring, Attack Detection and Mitigation"

Thursday 28 / Friday 29 September, 2006  
Tuebingen, Germany



## 1. VoIP Protocol

-- SIP: Session Initiation protocol

## 2. Attacks

## 3. High Speed Networks

## 4. Detection and Responses

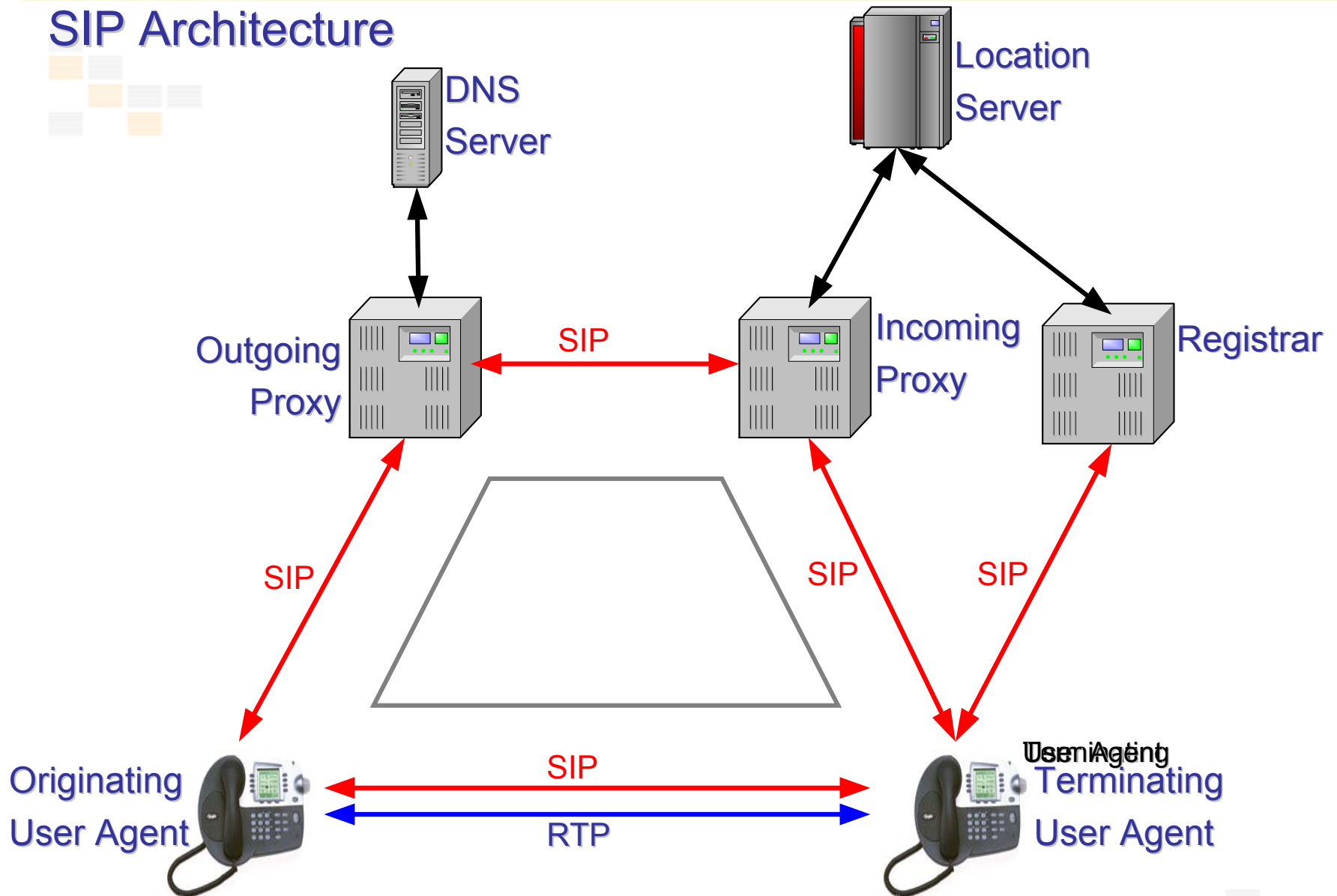


## SIP system components

1. User Agents
  1. Clients: Make requests
  2. Servers: Accept, reject and respond requests
  
2. Servers types
  - Redirect servers
  - Registrar servers
  - proxy servers
  - Location servers

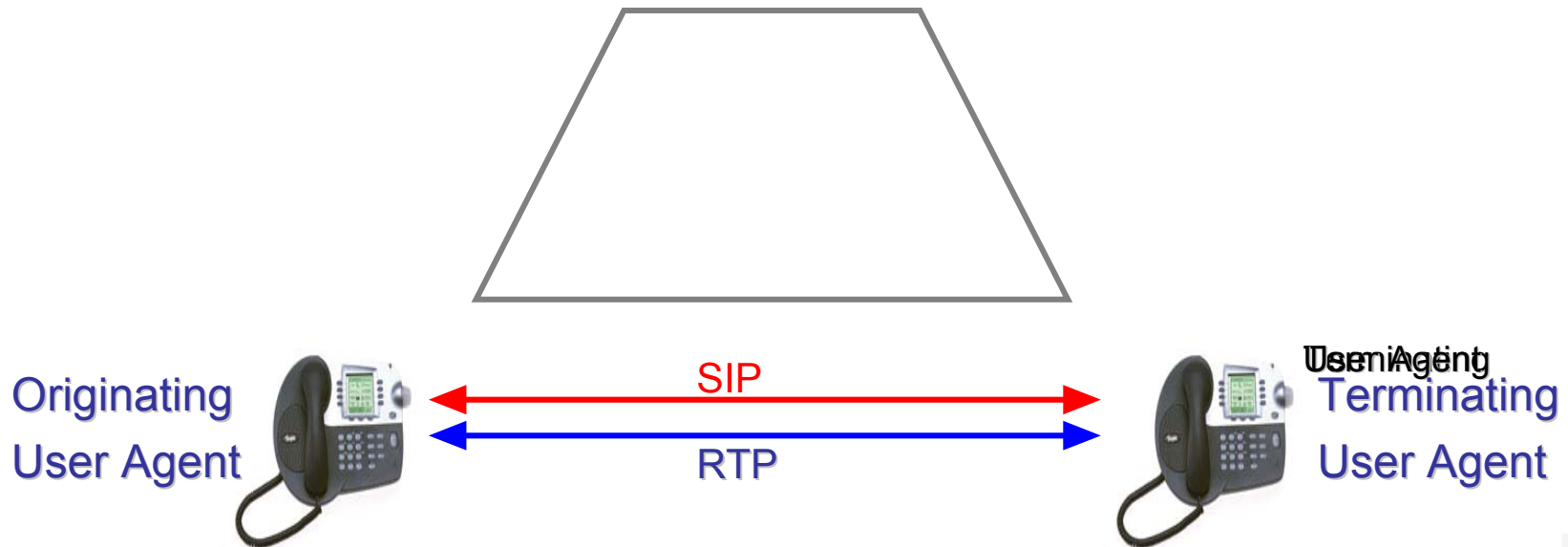
# SIP: Session Initiation Protocol

## SIP Architecture



# SIP: Session Initiation Protocol

## SIP Peer To Peer



## ■ Hijacking

### ▶ Registration hijacking

- ◆ Attacker registers under the identity of another user
- ◆ As a consequence the victim may no longer be able to register to the service neither pass nor receive calls
- ◆ Attacker may be able to pass or receive call under the victim identity

### ▶ Call hijacking

- ◆ Attacker establishes calls under the identity of another user

## ■ Service Theft

- ▶ Service theft consists in taking any unlawful benefit from a service
- ▶ Two cases are possible
  - ◆ Attacker with a VoIP account tries to
    - Get more bandwidth or QoS than subscribed
    - Add unauthorized media flows
    - Extend a call without being charged or call for free
  - ◆ Attacker without VoIP account tries to
    - Establish calls without being charged
- Denial of Service (DoS or DDoS)

## ■ Current Security SIP Mechanisms

### ▶ Protocol based

- ◆ HTTP Digest
- ◆ TLS
- ◆ IPSec
- ◆ ...

### ▶ Equipment based

#### ◆ Firewalls

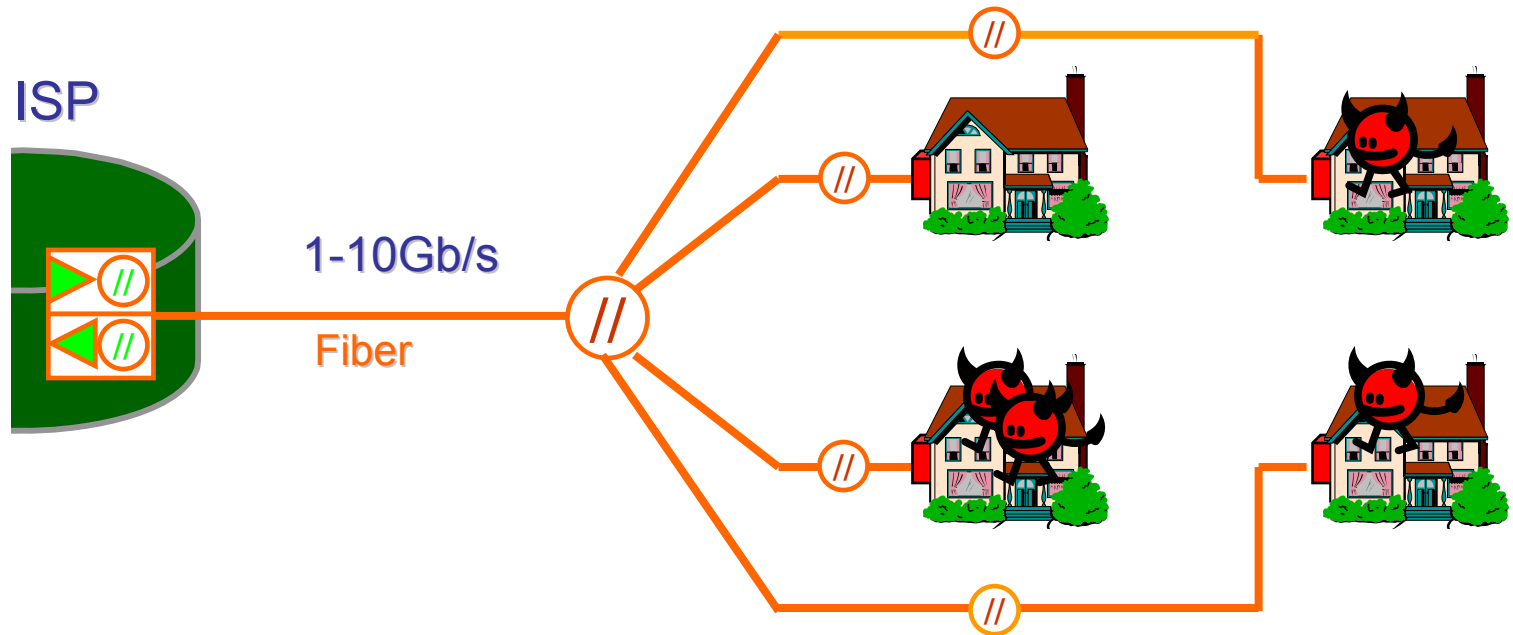
- Few firewalls implementation
- Stateless firewalls
- Limited packets inspection
- Cannot do anything against new attacks (Slammer 2003, ...)

#### ◆ IDS

- A few IDS products (early stage)

# High Speed Networks and monitoring

- ▶ Proliferation of broadband Internet
  - ◆ FTTH, GE-PON, etc...



# High Speed Networks and monitoring

---



- ▶ Need to monitor in this environment in the presence of new emerging services
- ▶ VoIP IDSs as a second barrier in this environment
  - ◆ Implementation of accurate VoIP IDSs
  - ◆ How to manage the huge amount of alerts?
  - ◆ Which points are more interesting to place these IDS tools?

# Questions?

---

