# TẤN CÔNG TỪ CHỐI DỊCH VỤ GIỮA CÁC SIP PROXY

***KS. Nguyễn Ngọc Quân***

*Tổ NCPT An toàn thông tin*

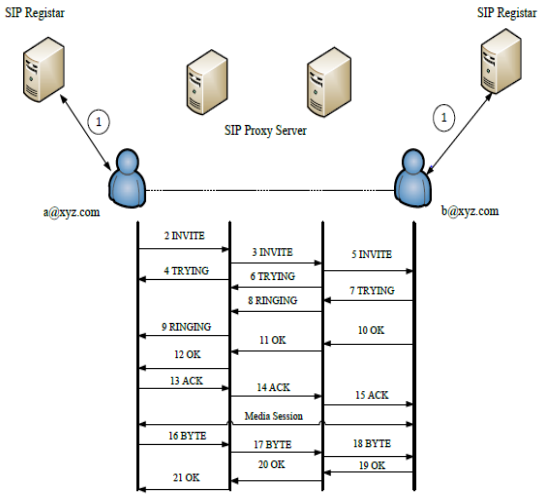
***Tóm tắt**: Hiện nay các dịch vụ thoại trên nền IP đang được phát triển mạnh mẽ và thay thế dần dịch vụ thoại truyền thống. Nhưng bên cạnh đó, những nguy cơ mất an ninh an toàn cũng đe dọa trực tiếp đến dịch vụ này. Trong bài báo này đề cập đến nguy cơ từ chối dịch vụ vào miền trunk của SIP. Về cơ bản kiểu tấn công này làm cho dịch vụ trở nên quá tải, người dùng gặp khó khăn trong việc gọi tới các thuê bao cần gọi. Bài báo này nêu lên một cách thức tấn công trong giao thức SIP và từ đó đưa ra những biện pháp, những khuyến nghị an ninh nhằm tăng cường bảo mật cho các nhà cung cấp dịch vụ VoIP.*

## 1. NGUYÊN LÝ HOẠT ĐỘNG CỦA SIP GIỮA CÁC SIP PROXY

Giao thức khởi tạo phiên SIP (Secssion Initiation Protocol) là giao thức điều khiển báo hiệu thuộc lớp ứng dụng được sử dụng để thiết lập, duy trì và kết thúc các phiên multimedia hay các cuộc gọi qua mạng nền IP. Các phiên làm việc cũng có thể là hội nghị đa phương tiện, cuộc gọi điện thoại điểm – điểm,…

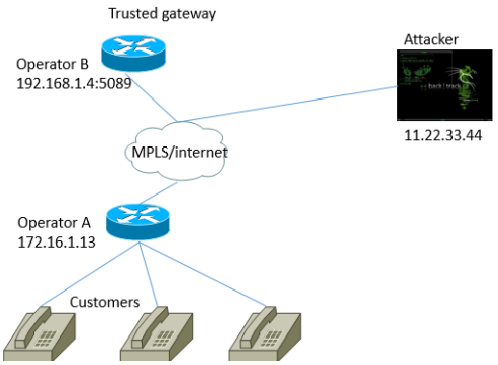
SIP Proxy (hay Proxy Server): có thể coi như các router thiết bị đầu cuối SIP mà chuyển tiếp các yêu cầu và trả lời. Vậy một trong những chức năng của Proxy Server là định tuyến.

Nhà cung cấp mạng thế hệ tiếp theo (NGN) cung cấp dịch vụ SIP tới khách hàng. Khách hàng có thể gọi khách hàng của nhà cung cấp mạng khác qua SIP Services và các SIP Gateways. Các SIP Gateways sử dụng SIP Trunks cho khởi tạo cuộc gọi đã được xác thực thực và tính cước. SIP Call Flow được thể hiện ở hình dưới:



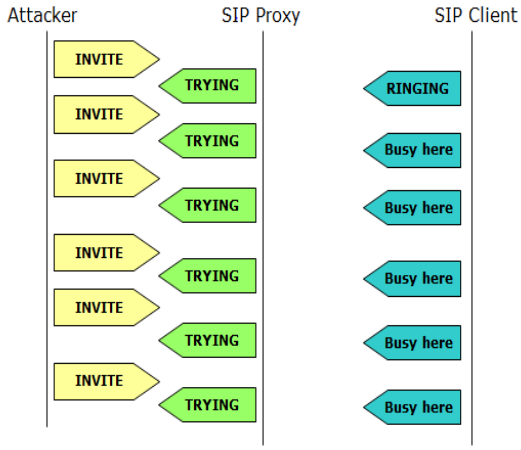

*Hình 1. SIP Call Flow*

Trong nhiều trường hợp, SIP trunk có thể được đại diện là 1 địa chỉ IP hoặc một "specific FROM number". Việc đáp ứng hoặc xác nhận chúng dựa trên sự xác thực là chậm đối với yêu cầu trong trường hợp này là đếm số cuộc gọi lớn. Bởi thế, các SIP trunk không có password hoặc không ứng dụng bộ lọc cơ sở IP cho sự xác nhận đường trunk. Các SIP trunk này sử dụng các "specific FROM numbers" hoặc Proxy Fields để khởi tạo 1 cuộc gọi. Bên cạnh đó hầu hết các đường trunks SIP có đặc quyền INVITE trực tiếp mà không cần REGISTER.




*Hình 2. Mô hình mạng mẫu cho NGN (mạng thế hệ tiếp theo) [1]*

Khi một bản tin INVITE được gửi để thiết lập cuộc gọi thì Proxy sẽ chuyển tiếp bản tin đó đồng thời duy trì kết nối cho sự thiết lập này cho đến khi kết nối bị hủy hoặc hết thời gian time out. Lợi dụng điều này Attacker có thể thực hiện tấn công bằng cách gửi nhiều bản tin INVITE giả mạo. Đích đến của các cuộc tấn công này là Proxy Server.




*Hình 3. Nguyên lý tấn công SIP Proxy*

Kết quả là Proxy còn "bận " chuyển tiếp các bản tin giả mạo dẫn đến làm giảm hiệu năng của các Proxy, tệ hơn có thể gây treo và phải khởi động lại.

## 2. CÁCH THỨC TIẾN HÀNH TẤN CÔNG TRÊN PHÂN ĐOẠN SIP TRUNK

Cách thức tiến hành có thể tổng kết lại như sau:

- Nhận 1 tài khoản (Account) hoặc cuộc gọi của khách
- Nhận 1 yêu cầu INVITE có sẵn.
- Kiểm tra cổng SIP đích cho INVITE Spoofing với tài khoản đã được biết.
- Gửi IP Spoofed INVITE Requests.
- Tạo mẫu INVITE Spoofing.
  - Địa chỉ IP cho vòng lặp (IP Addresses For Loop)
  - Số Port cho vòng lặp (Port Numbers For Loop)
  - Thay đổi biến INVITE (INVITE Variables) cho Spoofed IP Address and Port( địa chỉ IP và Port ảo)
  - Thiết lập trường FROM như IP:Port

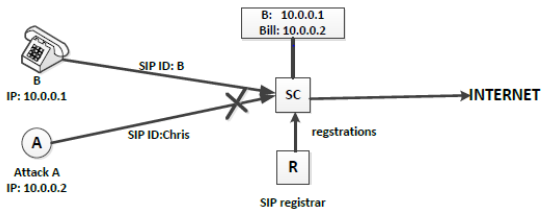
Cách thức tiến hành cụ thể được cho ở tài liệu *[1]*

**Hậu quả của việc tấn công từ chối dịch vụ SIP** trên phân đoạn SIP trunk làm cho SIP Proxy bị từ chối dịch vụ, không thể đáp ứng được các cuộc gọi của khách hàng. Tấn công từ chối dịch vụ gây ra việc mất uy tín của các nhà cung cấp dịch vụ đối với khác hàng, dù cho đằng sau nó là mục đích cạnh tranh hay phá hoại.

## 3. BIỆN PHÁP NGĂN CHẶN TẤN CÔNG

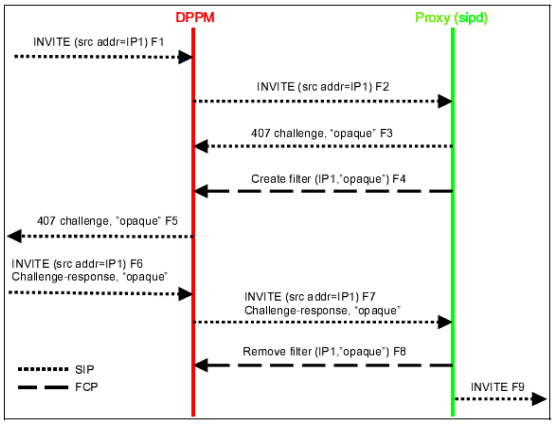
Anti – Spoofing: Bằng cách tạo ra danh sách các User hợp lệ có quyền truy cập. Mỗi User này được gán một giá trị Priority dựa vào địa chỉ IP nguồn. Ở đây sẽ có 2 hình thức để lựa chọn:

- Block tất cả các User không có giá trị Priority này truy cập vào, muốn truy cập thì các User phải đăng ký.
- Không Block các User này mà thực hiện xử lý theo cách sau: Ưu tiên chuyển tiếp các bản tin của các User có gán giá trị Priority.




*Hình 4 . Biện pháp Anti-Spoofing*

Yêu cầu xác thực: Lỗ hổng ở đây là các đường SIP trunks gửi bản tin INVITE trực tiếp mà không cần REGISTER. Chính vì vậy giải pháp được đưa ra là yêu cầu các đường này gửi bản tin INVITE đi kèm với việc xác thực User. Call Flow bây giờ trở thành:

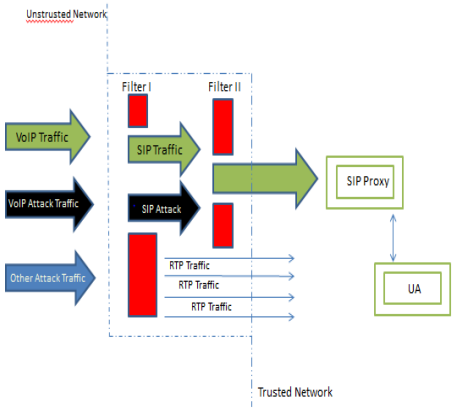



*Hình 5. Call Flow khi có xác thực [5]*

Sau khi nhận được bản tin INVITE, thay vì chuyển tiếp bản tin đó thì SIP Proxy gửi lại cho bên gửi bản tin 407 (Proxy Authentication Required) trong đó có mã xác thực trong trường Proxy-Authorization. Bản tin INVITE này chỉ được chuyển tiếp tới SIP Proxy khi chúng nhận được đúng mã xác thực tương ứng với địa chỉ IP nguồn.

- Ưu điểm: Đơn giản, tiết kiệm chi phí vì không phải cung cấp thiết bị của hãng thứ 3, việc xác thực đã có trong chuẩn.
- Nhược điểm: SIP Proxy ngoài chức năng định tuyến còn phải giải quyết vấn đề xác thực, vì vậy hiệu năng của thiết bị giảm ngay khi không bị tấn công.
- Nhận xét: Ngăn ngừa được hoàn toàn những user không được phép tấn công vào miền SIP Trunk.

Đề xuất được đưa ra ở đây là dùng các thiết bị chuyên dụng của hãng thứ 3. Các thiết bị này hoạt động trên nguyên lý chung là dùng các bộ lọc. Thường chúng ta sẽ dùng 2 bộ lọc lần lượt là lọc bản tin SIP rồi sau đó lọc các bản tin SIP hợp lệ



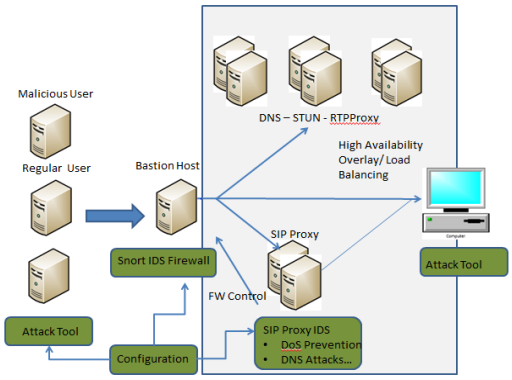

*Hình 6. Quy tắc sử dụng các bộ lọc [5]*

Kết quả thử nghiệm được cho trong bảng dưới đây: *[5]*

| Filters | Traffic Rate (CPS) | | | Avg CPU (%) |
|---|---|---|---|---|
| | Good | Spoof | Flood of Req | |
| Off | 240 | 800 | 800 | 85 |
| On | 240 | 7200 | 2400 | 42 |
| Off | 480 | 100 | 100 | 87 |
| On | 480 | 4800 | 2400 | 83 |

Các thiết bị lọc này thông thường là firewall, IDS với các lựa chọn là dùng riêng rẽ hay kết hợp cả hai. Firewall và IDS dùng các luật (rules) làm cơ sở cho các bộ lọc của chúng. Các biện pháp cụ thể được đưa ra là:

Thực hiện các chính sách về giám sát và lọc các bản tin SIP dùng IDS: duy trì các danh sách người dùng đáng ngờ làm cơ sở cho các quy tắc lọc. Các yếu tố mà có thể quyết định là xâm nhập trái phép dựa trên nguyên nhân gia tăng đột ngột lưu lượng đến Proxy hoặc các cuộc gọi xuất phát từ 1 User mà xác suất fail cao hoặc nội dung bản tin bị thay đổi đến máy chủ.

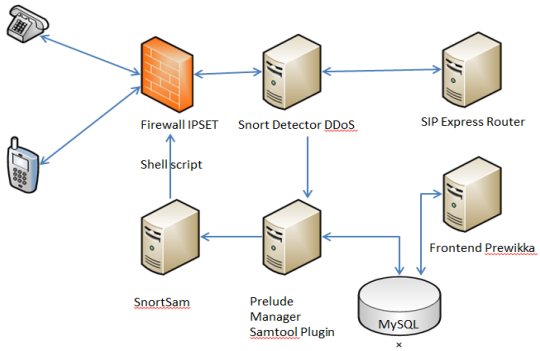



*Hình 7. Biện pháp sử dụng IDS [6]*

Dưới đây là ví dụ về một rules trong IDS:

Alert ip $ EXTERNAL_NET any -> $SIP_PROXY_IP $ SIP_PROXY_PORTS (msg: "TAN CONG DOS SIP TRUNK"; content:" INVITE"; depth:6; threshold: type both , track by_src, count 100, seconds 60; sid: 5000005; rev:1;

Triển khai bảo vệ theo nhiều lớp bằng cách đặt 1 firewall trước IDS. Mô hình sau có thể tham khảo:




*Hình 8. Biện pháp sử dụng IDS kết hợp Firewall [6]*

Kết quả thu được:

✓ Dựa trên việc lọc Packet: *[6]*

Số lượng packet sau firewall/ tổng số lượng packet =40%

✓ Dựa trên hiệu năng của thiết bị: *[5]*

| Traffic Composition | Firewall Filters OFF | | |
|---|---|---|---|
| | Good | Attack | CPU |
| | CPS | CPS | Load |
| | | | % |
| Non-Auth Traffic | 690 | 0 | 88 |
| Auth Good traffic | 240 | 0 | 20 |
| | 480 | 0 | 81 |
| Auth Good Traffic+ | 240 | 2950 | 84 |
| Spoof Traffic | 480 | 195 | 85 |
| Auth Good Traffic+ | 240 | 2970 | 87 |
| Flood of Req | 480 | 570 | 86 |
| Auth Good Traffic+ | 240 | 2970 | 87 |

Fillter on

| Traffic Composition | Firewall Filters ON | | |
|---|---|---|---|
| | Good | Attack | CPU |
| | CPS | CPS | Load |
| | | | % |
| Non-Auth Traffic | 690 | 0 | 88 |
| Auth Good traffic | 240 | 0 | 40 |
| | 480 | 0 | 82 |
| Auth Good Traffic+ | 240 | 16800 | 41 |
| Spoof Traffic | 480 | 14400 | 83 |
| Auth Good Traffic+ | 240 | 8400 | 41 |
| Flood of Req | 480 | 7200 | 83 |
| Auth Good Traffic+ | 240 | 8400 | 41 |

## 4. KẾT LUẬN

Thực tế chỉ ra rằng mặc dù tấn công DoS chỉ diễn ra trong thời gian ngắn nhưng hậu quả gây ra của nó rất nghiêm trọng. Bài báo đã giới thiệu một nguy cơ tấn công vào miền SIP trunk gây ra dạng tấn công DOS ATTACK và đưa ra một số biện pháp phòng ngừa. Đồng thời đưa ra một vài kết quả thử nghiệm để chứng minh điều này.

## 5. TÀI LIỆU THAM KHẢO:


1. *Hacking Trust Relationships of SIP Gateways, Fatih Özavcı.*
2. *Advanced Flooding Attack on a SIP Server, Xianglin Deng.*
3. *Protecting SIP against Very Large Flooding DoS Attacks, Felipe Huici, Saverio Niccolini, Nico d'Heureuse.*
4. *SIP INVITE Flood: Testing an Asterisk VoIP Server against a DDoS Attack, Eric Reeves, October 17, 2011.*
5. *Secure SIP: A Scalable Prevention Mechanism for DoS Attack on SIP Based VoIP Systems, Gaston Ormazabal, Sarvesh Nagpal, Edilon Yardeni, and Henning Schulzrinne.*
6. *Two layer Denial of Service prevention on SIP VoIP Infrastructures, Sven Ehlert, Ge Zhang, Dimitris Geneiatakis, Georgios Kambourakis, Tasos Dagiuklas, Jiri Mafkl, Dorgham Sisalem.*



**Thông tin tác giả:**

**Nguyễn Ngọc Quân**

**Sinh năm:** 1985

**Lý lịch khoa học:**

- Tốt nghiệp đại học kỹ thuật điện Quốc gia Saint Peterburgs, 2009, chuyên ngành khoa học máy tính.
- Hiện đang công tác tại Tổ NCPT An toàn thông tin thuộc Viện công nghệ Thông tin và Truyền thông – CDIT, Học viện Công nghệ Bưu chính Viễn thông.

**Lĩnh vực nghiên cứu hiện nay:** an ninh hạ tầng mạng, an ninh ứng dụng và bảo mật điện toán đám mây.

**Email:** quannn@ptit.edu.vn