Khoa Khoa học & Kỹ thuật máy tính
Trường ĐH Bách Khoa TP.HCM

Cryptography and Network Security
Lab 6
IP Security Protocol (IPSec)

Đặng Minh Việt 51204488
Trịnh Văn Quyền 51203042
Lê Tuấn Vũ 51204609

Task 1.2:

1.2.1. Explain the content of the two fields Initiator cookie and Responder cookie.

Hai thành phần tạo ra một số ngẫu nhiên được sử dụng cho mục đích chống tắc nghẽn. Những cookie này được dựa trên một định danh duy nhất cho mỗi peer (src và IP địa chỉ đích) và do đó bảo vệ chống lại các cuộc tấn công replay. Các ISAKMP RFC nói rằng phương pháp của việc tạo ra các cookie là thực hiện phụ thuộc nhưng đề nghị thực hiện một hash của nguồn và địa chỉ đích, nguồn và đích đến cổng UDP, một địa phương tạo ra ngẫu nhiên giá trị, thời gian, ngày tháng. Các cookie sẽ trở thành một định danh duy nhất cho phần còn lại của các thông điệp được trao đổi trong IKE.

Generation of the Initiator cookie: An 8-byte pseudo-random number used for anti-clogging

CKY-I = md5{(src_ip, dest_ip), random number, time, and date}

Generation of the Responder cookie: An 8-byte pseudo-random number used for anti-clogging

CKY-R = md5{(src_ip, dest_ip), random number, time, and date}.

1.2.2.Observe the cookies from the 2nd ISAKMP message. Explain your observation.

Sending Message 1:

ISAKMP header- Các tiêu đề ISAKMP chứa cookie của người khởi xướng, và cookie của người trả lời là trái số 0 cho trả lời để tính toán và điền vào.

Sending Message 2

ISAKMP header- Bạn có thể thấy rằng các tiêu đề ISAKMP bây giờ có cả hai lĩnh vực Cookie thiết lập để các giá trị tương ứng: Initiator cookie and Responder cookie.

1.2.3. If the AH protocol is used in the transport mode, can you read the content of the protected IP packets? How about the ESP protocol? Explain your answer.

Các tiêu đề AH được chèn vào các gói tin giữa IP header và dữ liệu.Dữ liệu sẽ được mã hóa còn IP header thì không. IP header kẻ xâm nhập có thể đọc được nhưng dữ liệu thì không.

ESP cung cấp xác thực, tính toàn vẹn và tính bí mật, nhằm chống lại các dữ liệu giả mạo và cung cấp bảo vệ nội dung tin nhắn.ESP cũng cung cấp tất cả các dịch vụ mã hóa trong IPSec. Mã hóa / giải mã cho phép chỉ người gửi và người nhận ủy quyền để đọc dữ liệu. Ngoài ra, ESP có một tùy chọn để thực hiện xác thực, được gọi là ESP xác thực. Sử dụng ESP xác thực, ESP cung cấp xác thực và toàn vẹn cho dữ liệu và không dùng cho các IP header. Các tiêu đề ESP được chèn vào các gói tin giữa IP header và dữ liệu.

1.2.4. Extract the AH header from a IPSec protected IP packet. Explain the role of each of the files from the AH header.

Next Header (8 bits): chỉ ra những giao thức tầng trên được bảo vệ.

Payload Len (8 bits): chiều dài của AH.

Reserved (16 bits): Dự trữ để dùng trong tương lai .

Security Parameters Index (32 bits): Giá trị tùy ý mà được sử dụng (cùng với địa chỉ IP đích) để xác định sự liên kết an ninh của bên nhận.

Sequence Number (32 bits): tăng lên 1 đơn vị để ngăn chặn tấn công replay.

Integrity Check Value (multiple of 32 bits): Biến giá trị kiểm tra chiều dài.