http://dx.doi.org/10.5392/JKCA.2013.13.04.017

위치 정보 서버를 이용한 SIP 위장공격 대응 방안

Countermeasure of SIP Impersonation Attack Using A Location Server

고윤미, 권경희
단국대학교 전자계산학과 컴퓨터과학

Yun-Mi Go(alice8105@dankook.ac.kr), Kyung-Hee Kwon(khkwon@dankook.ac.kr)

요약

SIP의 보안 취약점을 이용한 위장공격은 공격자로 하여금 과금 회피, 세션 가로채기를 용이하게 하여 사용자에게 피해를 줄 수 있으므로 이에 대한 대응 방안이 요구된다. 따라서 본 연구에서는 위장공격을 탐지하기 위한 새로운 기법을 제안한다. 등록 서버는 전송된 레지스터 요청 메시지의 헤더 값 중 From 또는 Call-ID값을 포함한 레코드가 위치 정보 서버에 저장되어 있는지 확인한다. 만약 저장된 레코드가 존재하고 그 값이 주기적으로 갱신된다면 등록 서버는 전송된 레지스터 요청 메시지를 위장공격으로 판별하여 요청 메시지를 무시한다. 이 기법은 위장 공격을 방어하기 위해 사용자 인증을 위한 암호화 메커니즘을 추가하는 형태가 아닌 위치 정보 서버에 저장된 정보를 이용하여 보다 안전한 SIP 환경을 쉽게 구축할 수 있다.

■ 중심어 : | SIP | 위장공격 | 등록 요청 메시지 | 위치 정보 서버 |

Abstract

Impersonation attack, based on vulnerable security of SIP, facilitate a intruder to take malicious actions such as toll fraud and session hijacking. This paper suggests a new technique for a countermeasure. When receiving a register request message, registrar checks whether the value of Form header or the value of Call-ID header is stored in location server or not. If the record containing either of them are stored and periodically updated, we regard that message as impersonation attack and discard it. Since this technique uses the information stored in server instead of adding encryption mechanism for user authentication, it can easily build securer SIP environment.

■ keyword : | SIP | Impersonation Attack | Register Request Message | Location Server |

I. 서 론

VoIP(Voice Over Internet Protocol)[1]서비스는 IP망을 이용하여 음성 데이터를 전송하는 기술로서 인터넷 망에 접속 가능한 장소 어디에서든지 저렴한 통신비용으로 음성 전화 서비스를 이용할 수 있다는 편리함을 가지고 있다. 그러나 VoIP 서비스에 이용되는 SIP 프로토콜의 취약점으로 인해 비정상 메시지 공격, 서비스 거부 공격, 도청, 위장공격 등의 위협이 발생하고 있다[2][3].

이러한 이유로 현재 SIP 프로토콜의 위협을 개선하기 위한 연구들이 활발히 진행되고 있다. 특히 공격자가 패킷 스니핑을 통해 획득한 정보를 이용하여 정상적인 사용자로 위장한 공격 대응 방안으로는 사용자 인증

접수번호 : #130212-004
접수일자 : 2013년 02월 12일
심사완료일 : 2013년 04월 08일
교신저자 : 고윤미, e-mail : alice8105@dankook.ac.kr

을 강화하는 여러 암호화 기법들이 있다. 그러나 기존의 제안된 방법들은 보안상 취약점을 가지고 있거나 잦은 인증 키 교환과정에서 생기는 추가적인 오버헤드로 인해 서비스 지연이라는 문제점이 발생한다.

이에 본 논문에서는 위장 공격 시 기존 대응방안의 문제점들은 보안하기 위해 위치 정보 서버(Location Server) 에 저장된 정보를 이용하여 공격자를 탐지하고 차단하는 방식을 제안하였다. 즉, VoIP 서비스를 이용하기 위해 공격자는 등록 서버에 레지스터 요청 메시지를 전송한다. 이때 등록 서버는 레지스터 요청 메시지를 전송한 단말(SIP User Agent) 정보가 현재 위치 정보 서버에 저장되어 있는지 확인한다. 만약 저장된 정보가 주기적으로 갱신되고 있을 경우 현재 레지스터 요청 메시지는 공격자가 전송한 것으로 판별하고 이를 차단하여 공격자를 대응한다.

본 논문의 구성은 다음과 같다. 2장에서는 SIP 보안 기법들을 분류하고 각 기법들에 대한 취약점을 분석한다. 3장에서는 위장 공격 탐지 메커니즘을 제안한다. 마지막으로 4장에서는 결론을 제시하였다.

II. 관련연구

위장공격은 인증 받지 않은 사용자가 정상적인 사용자로 위장하여 서비스를 불법적으로 이용하는 것으로 과금회피, 세션 가로채기가 가능하다. 실제 공격자가 정상적인 사용자의 SIP URI와 패스워드를 유추하고 이를 이용하여 불법적으로 음성 전화 서비스를 받아 금전적 피해를 입힌 사례도 있다. 현재 위장공격 대처 방안으로는 사용자 인증을 위한 보안 메커니즘이 사용되고 있다.

IETF SIP[4] 표준에서는 사용자 인증과 SIP 메시지를 보호하기 위하여 HTTP Digest 인증기법 , TLS (Transport Layer Security), IPsec, S/MIME(Secure /Multipurpose Internet Mail Extension)보안 프로토콜을 사용한다. HTTP Digest 인증 기법은 메시지에 대한 인증과 재사용(replay)공격을 방지하지만 메시지에 대한 무결성이 보장되지 않는다. 더욱이 기존의 HTTP Digest는 Challenge-Response 방식을 사용하고 있기 때문에 사전에 공유된 패스워드를 제외한 나머지 값들이 공격자에게 쉽게 노출되어 패스워드 유추가 가능하다. 이에 홉 간의 보안 기술인 TLS을 동시에 사용하여 안전한 인증 서비스를 제공한다. TLS는 SIP 메시지에 대한 암·복호화를 통해 홉 간의 보안채널을 형성하기 때문에 메시지의 무결성과 기밀성이 제공된다.

S/MIME프로토콜은 SIP 사용자간의 보안 기능을 제공하여 사용자 인증, 메시지의 무결성, 기밀성을 제공한다. 그러나 표준에서 정의한 TLS, S/MIME 보안 프로토콜들은 PKI(Public Key Infrastructure) 기반의 보안 프로토콜이기 때문에 PKI 환경이 구축되지 않은 환경에서는 적용할 수 없다. 더욱이 많은 메시지 교환과 암호학적 연산량을 요구하는 TLS 보안 프로토콜은 성능 문제로 실제 네트워크에 적용하기 어렵다.

또한 메시지 교환 시 인증키를 갱신하는 방법[5-8], SIP 메시지의 상태 정보와 서버 사이의 인증 통한 방법[9], SIP 등록 서버(Registrar)에 등록 시에 주고받는 메시지들의 시간 정보를 이용하여 일회용 패스워드를 생성하고 이를 이용하여 사용자 인증을 강화한 기법[10] 등이 제안되었다. 그러나 이러한 기법들은 인증키 교환 과정에서 생기는 추가적인 오버헤드로 인해 시스템의 부하를 증가시키게 되는 단점이 있다.

따라서 본 논문에서는 기존 방안들의 문제점을 해결하기 위해 위장공격에 대해서 분석하고 이를 탐지하고 방어할 수 있는 방안을 연구하였다.

III. 제안하는 메커니즘

SIP 프로토콜은 취약한 인증구조와 SIP 패킷 정보를 쉽게 취득할 수 있는 특성 때문에 정상적인 사용자로 위장하는 공격이 용이하다. 더욱이 위장공격은 사용자들의 금전적 피해와 통화 방해로 사용자에게 큰 불편을 줄 수 있는 공격이므로 이에 대한 대응 방법이 요구된다. 이에 본 논문에서는 암호와 메커니즘을 이용하여 사용자 인증을 강화하는 기존 방식과 달리 위치 정보 서버에 저장된 정보를 이용하여 공격자를 판별하는 방안을 제시하고자 한다.

본 연구에서는 오픈 소스로 공개된 OpenSIPS 1.71을 이용하여 서버를 구축하고 wireshark1.6.2와 x-lite 4 소프트 폰을 이용하여 위장공격을 [그림 1]과 같이 시도하였다

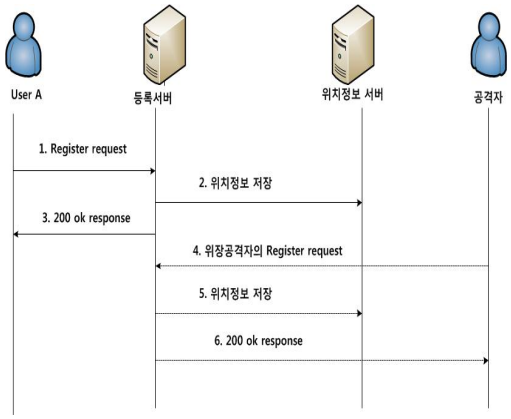

그림 1. 위장공격 과정

[그림 1]은 위장공격 과정으로 공격자는 정상적인 사용자의 레지스터 메시지를 스니핑한 후 이를 이용하여 등록 서버에게 위조된 레지스터 메시지를 전송한다. 위조된 레지스터 메시지의 To, From, SIP URI, 인증 패스워드는 정상적인 사용자와 동일하기 때문에 위조된 메시지를 수신한 등록서버는 공격자를 정상적인 사용자로 인식하여 위치정보 서버에 정보를 저장한다. 이때 저장되는 정보의 값들은 [표 1]과 같다. 그 후 공격자는 정상적인 서비스를 받을 수 있게 되며 인터넷 전화 이용 시, 과금을 회피할 수 있게 된다. 또한 공격자가 정상적인 SIP 단말보다 우선순위가 높게 되어있을 경우에는 정상적인 사용자의 호 설정 세션을 가로 챌 수 있다. 위조된 레지스터 메시지의 사용되는 To 값은 수신자의 이름과 <> 안에 표시되는 수신자 URI이고, From 값은 요청자의 이름과 <>안에 표시되는 요청자 URI이다.

등록 서버는 레지스터 요청 메시지의 Contact, Call-ID, Cseq , Expires 값을 이용하여 위치정보를 등록 하거나 갱신 또는 삭제하게 된다. SIP 단말은 위치 지정 서비스를 받기 위해 등록 서버에게 동일한 Call-ID로 레지스터 요청 메시지를 주기적으로 전송하여 세션을 유지한다. Call-ID는 난수로 생성된 문자열로 같은 세션동안은 변경되지 않는 특징이 있다. 하지만 정상적인 SIP 단말의 레지스터 요청 메시지일지라도 SIP 단말이 전원을 다시 켰을 때, 같은 SIP URI와 인증 패스워드를 다른 단말에서 사용할 때 레지스터 요청 메시지의 Call-ID와 Contact 값이 변경된다. 또한 SIP 단말이 이동하였을 때 레지스터 요청 메시지의 Contact값이 변경된다. 이에 공격자가 정상적인 사용자와 똑같은 To, From, SIP URI, 인증 패스워드를 이용하여 레지스터 요청 메시지를 전송할 때 Call-ID또는 Contact 값이 변경되어도 정상적인 사용자로 분류되어 등록 서버는 위치 정보 서버에 정보를 등록 하게 된다.

표 1. Location 정보

이름	내용
id	DB의 고유 ID
username	레지스터 요청 메시지의 SIP의 전화번호, From 헤더의 요청자 이름
domain	레지스터 요청 메시지의 도메인
contact	레지스터 요청 메시지의 contact 헤더 필드의 값인 SIP URI.
received	전송받은 IP: PORT
path	레지스터 요청 메시지의 path 헤더 rfc 3327
expires	레지스터 요청 메시지의 만료시간
q	우선시되는 라우팅 값
call-id	레지스터 요청 메시지의 call-id 헤더 필드의 값
cseq	레지스터 요청 메시지의 cseq 헤더 필드값
last_modify	마지막 레지스터 요청 메시지 도착시간

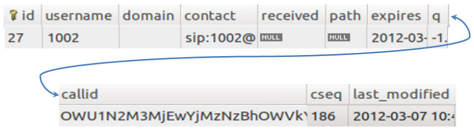

그림 2. 위장 공격 전 Location DB

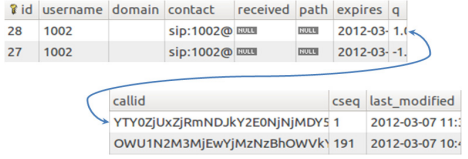

그림 3. 위장 공격 후 Location DB

[그림 2]과 [그림 3]는 실제 위장 공격 시 위치 정보 서버의 변화된 값으로 [그림 3]은 위장공격이 이루어지기 전 위치 정보이며, [그림 4]는 공격자가 정상적인 SIP 단말로 위장하여 등록 서버에 레지스터 요청 메시지를 전송한 후 위치 정보 서버에 저장된 정보이다.

이에 본 논문에서는 보안메커니즘을 추가하여 공격을 탐지 하는 방식이 아닌 등록 서버에서 레지스터 요청 메시지를 수신하였을 때 [그림 5]의 점선 부분을 추가하여 정상적인 사용자와 위장 공격자를 판별한다.

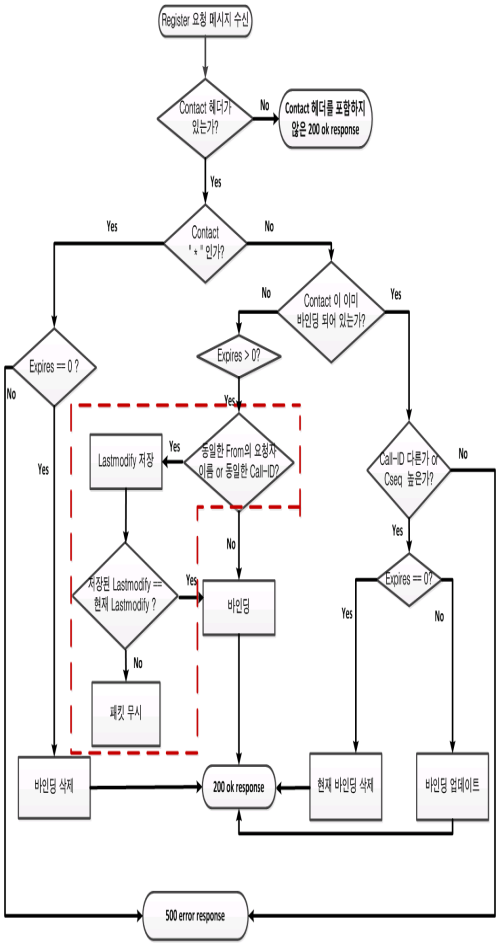

그림 4. 등록서버에서 위장공격을 탐지하고 방어하는 순서도

등록 서버는 수신된 레지스터 요청 메시지의 Contact 값이 이미 바인딩 되어있는지 먼저 확인한다. Contact 값이 이미 바인딩 되어 있지 않고 수신된 레지스터 메시지의 From 헤더의 요청자 이름과 동일한 Username, Call-ID가 위치 정보 서버에 저장되어 있지 않을 경우 정보를 위치 정보 서버에 등록 하고 등록 서버는 200 ok 레지스터 응답 메시지를 전송하여 정상적인 서비스를 받을 수 있게 한다. 만약 그렇지 않을 두 가지 경우 정상적인 사용자인지 공격자인지 판별해야하며 두 가지 경우는 다음과 같다.

첫 번째 레지스터 요청 메시지 From 헤더의 요청자 이름은 같고 Contact와 Call-ID가 상이할 경우는 사용자가 전원을 다시 켰을 때와 정상적인 사용자가 동일한 SIP-URI와 인증 패스워드를 이용하여 다른 기기에서 서비스를 받고자 할 때 또는 위장공격일 때 이다. 두 번째 레지스터 요청 메시지 From 헤더의 요청자 이름과 Call-ID는 동일하고 Contact 이 상이할 경우는 정상적인 사용자가 현재 세션을 유지하면서 이동하거나 동일한 Call-ID를 이용한 위장공격 때 이다. 이러한 두 가지 경우 공격자를 판별하기 위해 다음과 같은 과정이 이루어진다.

첫 번째, 등록 서버는 수신된 레지스터 요청 메시지 From 헤더의 요청자 이름 또는 Call-ID가 동일한 정보가 위치 정보 서버에 존재 하는지 확인한다.

두 번째, 만약 위치 정보 서버에 존재할 경우 last_modify 값을 저장한다. 그렇지 않을 경우 등록 서버는 수신된 레지스터 요청 메시지의 정보를 위치 정보 서버에 저장한다.

세 번째, 만약 last_modify 값을 저장 하였다면 주기 시간 후 저장된 last_modify 값과 현재 위지 정보 서버에 저장된 last_modify값을 비교한다.

네 번째, last_modify 값이 상이할 경우 저장된 정상적인 사용자가 세션을 유지하고 있으므로 수신된 레지스터 요청 메시지는 공격자에 의해 전송된 것으로 판단한다. 정상적인 사용자는 등록 서버에게 레지스터 요청 메시지를 주기적으로 전송하기 때문에 주기시간 마다 last_modify 값이 변경된다. 따라서 last_modify 값이 상이할 경우 수신된 레지스터 요청 메시지는 공격자에 의해 전송된 것이므로 등록 서버는 현 요청 메시지를 위치 정보 서버에 등록하지 않고 응답 메시지 또한 전

송하지 않는다. 그 결과 공격자는 정상적인 서비스를 이용하지 못하고 차단된다.

last_modify 값이 동일한 경우 정상적인 사용자가 세션을 유지하고 있지 않으므로 정상적인 사용자가 SIP 단말의 전원을 다시 켰을 때 또는 정상적인 사용자가 다른 단말을 이용할 경우 또는 SIP 단말이 이동한 경우로 판단 할 수 있다. 그러므로 등록 서버는 전송된 현 요청 메시지를 이용하여 위치 정보 서버에 정보를 등록하고 200 ok 응답 메시지를 전송하여 정상적인 서비스를 받을 수 있게 한다.

본 논문에서 사용되고 있는 주기 시간은 단말과 등록 서버의 세션을 유지하기 위해 단말이 전송하는 레지스터 요청 메시지의 시간 간격을 의미한다. 이 주기 시간은 SIP 단말마다 다르며 국내에서 상용되어 사용되어지고 있는 SIP 단말의 주기시간은 30초 내외이며, 본 논문에서 사용되고 있는 소프트 폰은 주기시간이 60초 내외이다.

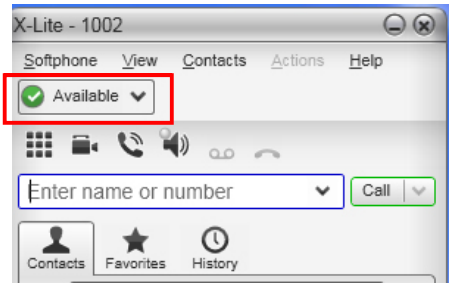

그림 5. 등록 서버에 위장공격 시 공격자 소프트 폰 상태

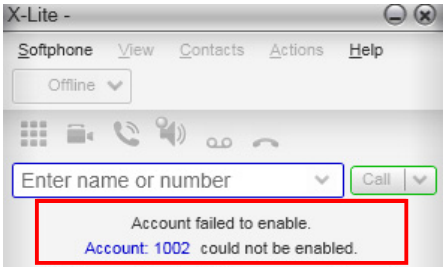

그림 6. 제안한 메커니즘을 적용한 등록 서버에 위장공격 시 공격자 소프트 폰

본 논문에서 제안한 메커니즘을 사용하였을 경우 위장 공격 시 위치 정보 서버의 정보는 [그림 2]와 같았다. 즉 위장 공격을 탐지하여 위치 정보 서버에 정보를 등록하지 못하고 있음을 알 수 있다. [그림 5]은 위장공격이 이루어 졌을 때 공격자의 소프트 폰 상태 이다. 즉, 등록 서버는 위장 공격자를 탐지 못하기 때문에 위치 정보 서버에 정보를 등록한 후 정상적인 서비스를 받을 수 있게 된다. [그림 6]은 제안한 위장공격 탐지 기법에 의해 차단된 공격자의 소프트 폰 상태이다. 즉, 등록 서버는 위장공격자를 탐지하고 등록 요청 메시지를 무시하기 때문에 공격자는 응답 메시지를 수신하지 못하게 된다. 그 결과 공격자는 정상적인 서비스를 이용할 수 없게 차단되었다.

본 논문에서는 위장공격을 방어하기 위해 사용자 인증을 강화하는 보안메커니즘을 사용하지 않고도 현재 위치 정보 서버에 저장된 값만을 이용하여 위장공격을 손쉽게 방어할 수 있게 되었다. 더욱이 제안한 메커니즘은 보안 강화를 위해 추가된 메시지가 없고 몇 번의 비교만으로 공격자를 판별하기 때문에 기존의 방식인 암호화 기법의 문제점을 해결할 수 있게 되었다. 또한 제안한 메커니즘은 기존 등록 서버의 역할인 새로운 UA의 등록, 수정, 삭제 과정이 동일하게 이루어지기 때문에 등록 서버의 성능을 저하시키지 않고 위장 공격을 판별할 수 있었다.

Ⅳ. 결론

VoIP는 편리함과 저렴한 통신비용의 장점으로 사용자들에게 빠르게 보급되고 있다. 그러나 VoIP에서 사용되는 SIP 프로토콜은 취약한 인증구조와 SIP 패킷 정보를 쉽게 취득할 수 있는 특성으로 인해 위장 공격이 이루어 질 수 있다. 위장 공격은 과금을 회피할 수 있을 뿐만 아니라 정상적인 사용자의 세션을 가로채기 가능하다. 이에 위장 공격을 탐지하고 방어하는 메커니즘이 필요한 실정이다. 본 논문에서는 정상적인 사용자에 의해 저장된 정보를 이용하여 위장 공격자를 판별하는 메커니즘을 제안하였다. 즉, 정상적인 사용자에 의해

주기적으로 전송되는 레지스터 요청 메시지를 통해 현재 전송된 레지스터 요청 메시지가 공격자에 의해 전송된 메시지인지를 판별한다. 이 기법은 추가적인 인증과정을 거치지 않고도 최소한의 오버헤드를 이용하여 보안 기능을 강화하였다.

참 고 문 헌

[1] 한국전자통신연구원(ETRI) 기술 평가팀, "*VoIP 기술 및 시장 동향*", 한국전자통신연구원(ETRI) 2006.

[2] Keromytis and D. Angelos, "A Comprehensive Survey of Voice over IP Security Research," Communication Surveys & Tutorials, IEEE, Issue:99, pp.1-24, 2011(4).

[3] A. D. keromytis, "Voice over IP Security: Research and Practice," IEEE Security Privacy Mag, Vol.8, pp.76-78, 2010(3/4).

[4] Rosenberg, H. Schulzrinne, G. Camarillo, A. Johnston, J. Peterson, R. Sparks, M.handley, and E. Schooler, "SIP: Session Initiation Protocol," RFC 3261, 2002(1).

[5] 최재덕, 정수환 "효율적이고 안전한 SIP 사용자 인증 및 키 교환", 한국정보보호학회논문지, 제19권, 제3호, 2009(6).

[6] P. Thermos, *"Two Attacks against VoIP,"* SecurityFocus, 2006(4).

[7] R. Srinivasan V. Vaidehi K. Harish, K. Lakshmi-Narasimhan, S. LokeshwerBabu, and V. Sirkanth, "Authentication of Signalling in VoIP Applications," Communication, Asia-Pacific Conference, pp.530-533, 2005(10).

[8] C. H. Wang and M. W. Li "A Distributed Key Changing Mechanism for Secure Voice-Over-IP Service," 2007 IEEE International Conference on Multimedia and Expo, 2007.

[9] 윤하나, 이형우, "SIP 공격 대응을 위한 보안성이 강화된 Stateful SIP 프로토콜," 한국콘텐츠학회논문지, 제10권, 제1호, 2010(1).

[10] 고윤미, 권경희, "SIP에서의 강화된 사용자 인증 방식", 한국콘텐츠학회논문지, 제11권, 제2호, 2011(12).

저 자 소 개

고 윤 미(Yun-Mi Go) 정회원

- 2004년 : 단국대학교 전자계산학과(이학사)
- 2007년 : 단국대학교 전자계산학과 컴퓨터과학(이학석사)
- 2008년 ~ 현재 : 단국대학교 전자계산학과 컴퓨터과학(박사과정)

<관심분야> : 컴퓨터 네트워크, 네트워크 보안

권 경 희(Kyung-Hee Kwon) 정회원

- 1976년 : 고려대학교 물리학과(이학사)
- 1986년 : Old Dominion Univ. Dept. of Computer Science(M.S.)
- 1992년 : Louisiana State Univ. Dept. of Computer Science(Ph.D)
- 1979년 ~ 1984년 : 산업연구원(KIET) 연구원
- 1993년 ~ 현재 : 단국대학교 교수

<관심분야> : 컴퓨터 네트워크, 알고리즘 분석 및 설계, 네트워크 보안