네트워크 트래픽의 은닉채널에 관한 연구

손태식[0], 서정우*, 서정택**, 문종섭*
*고려대학교 정보보호기술연구센터, **국가보안기술연구소
{743zh2k[0], korea, jsmoon}@korea.ac.kr, seojt@etri.re.kr

A Study on the Analysis of Covert Channel in Network Traffic

Tae-Shik Sohn[0], Jung-Woo Seo*, Jung-Taek Seo**, Jong-Sub Moon*
*CIST Korea Univ, ** NSRI

요 약

은닉채널에 관한 연구는 1980년대 이전부터 진행되어 왔으며, 최근에는 멀티미디어 데이터에 대한 스테가노그래피에 대한 관심이 집중되고 있다. 하지만, 본 논문에서는 현재 스테가노그래피나 정보은닉에서 다루는 동영상 데이터에 대한 은닉채널이 아닌, 인터넷 환경의 근간을 이루는 TCP/IP 네트워크 트래픽에 존재하는 은닉채널에 대한 연구를 수행하였다. 먼저 은닉채널 개념 및 기존 연구동향을 분석하였으며, 그 후 TCP/IP를 구성하는 각 프로토콜에 생성 가능한 은닉채널을 분석하여 향후 연구 방향을 제시하였다.

1. 서론

네트워크 환경의 급속한 발달과 함께 네트워크를 통해 전달되는 정보 혹은 네트워크 환경에 포함된 정보의 양은 점점 더 증가하고 있다. 이러한 정보의 증가는 네트워크 자원에 대한 보안 문제로 연결되며 지금 이 순간에도 우리는 네트워크의 취약성을 이용한 여러 공격이나 컴퓨터 바이러스에 노출되어 있다. 하지만, 앞서 열거된 공격들에 대한 대응을 위한 해결책으로 방화벽, IDS, 안티-바이러스 솔루션 등의 대응 방안이 제안되고 있지만, 이러한 솔루션은 물론이고 현재 네트워크 환경의 근간인 TCP/IP 프로토콜의 내재된 취약성을 이용한 공격에 대해서는 특별한 대응책을 가지고 있지 못하다. TCP/IP 프로토콜은 기본적으로 효율중심의 프로토콜로서 개발 당시에는 보안적인 측면에 대한 고려가 전무했다. 그러므로 TCP/IP를 구성하는 여러 프로토콜들 및 그 응용 서비스들을 이용하여 일반 네트워크 트래픽처럼 보이는 은닉 채널을 생성이 가능하다. 즉, 보안 솔루션들로 보호되는 네트워크일지라도 은닉채널을 통해 내부로부터의 정보 누출이 가능한 것이다. 여기서 은닉 채널이란 시스템의 보안 정책을 위반하는 어떤 방법을 사용하여 정보를 전송하는 프로세스에 의해 이용될 수 있는 임의의 통신 채널로서 정의 할 수 있다. 근본적으로 이와 같은 통신 채널은 일반적인 컴퓨터 설계상의 통신 수단이 아니며 보통 특정 정보에 접근하는 것이 허락되지 않는 프로세스나 사용자들에게 정보를 전송하기 위한 수단으로서 사용된다[1].

본 논문에서는 은닉채널이라 불리는 두 호스트간 기밀통신 채널의 개념과 관련 연구 동향을 파악한 후, TCP/IP 프로토콜에서 생성 가능하다고 알려진 여러 은닉 채널 형성 방법을 분석하였다.

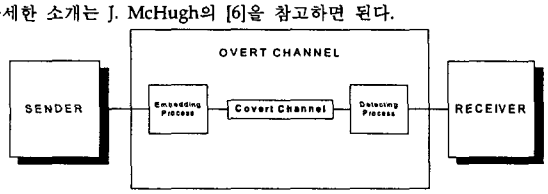
2. 은닉채널

2.1 은닉채널 소개

은닉채널 기법을 분석하기 전에 먼저 은닉채널의 개념과 종류 등에 대해서 알아보겠다.

은닉채널은 그림 1과 같이 공개채널(Overt Channel)과 구분되어 정의될 수 있다[2]. 은닉채널에서는 데이터를 전송하기 위해 일반적인 통신 채널 즉, 공개채널을 사용하지만 이때 일반 통신채널 속에 포함된 특정 데이터에 대한 은닉화 기법은 은닉채널의 생성자 외에는 알 수 없다. 하지만, 공개채널에서는 은닉채널과 마찬가지로 일반적인 통신채널을 이용하지만, 데이터의 기밀성을 유지하기 위한 기법이 공개되거나 쉽게 구분이 될 수 있는 차이점을 가지고 있다.

은닉채널이란 용어는 Lampson의 [3]에서 처음으로 소개되었으며, 그 개념에 대한 정의는 1985년의 미국 DOD의 기술문서 [1]에 잘 나타나 있으며, 그 정의는 "Any communication channel that can be exploited by a process to transfer information in a manner that violates the systems security policy"이다. 또한 유사한 의미로 steganography, information hiding, subliminal channel 등이 사용된다. 은닉채널은 보통 은닉저장채널(Covert Storage Channel)과 은닉시간채널(Covert Timing Channel)로 구분한다. 은닉저장채널은 임의의 프로세스가 특정 오브젝트의 값을 변경하게 되면 다른 프로세스는 그러한 오브젝트 값 변경의 결과를 관찰하여 특정 정보를 알아낼 수 있는 임의의 통신 채널을 말한다. 또한 은닉시간채널은 임의의 프로세스가 CPU, I/O 등 시스템 자원에 대한 어떤 효과를 유발하게 되면 그 결과가 상대 프로세스에 의해 관찰되고 이렇게 관찰된 시간을 바탕으로 특정 정보를 알아낼 수 있는 채널이다[4][5]. 은닉채널 자체에 대한 보다 자세한 소개는 J. McHugh의 [6]을 참고하면 된다.



[그림 1] 공개 채널과 은닉채널과의 관계

2.2 은닉채널 연구 동향

은닉채널에 관한 연구는 1970~80년대에 [1-6]과 같이 은닉채널의 개념 형성 및 정의에 관한 연구를 시작으로 최근에는 멀티미디어 데이터에 대한 정보 은닉(Information Hiding)분야에서 활발하게 그 연구가 진행되고 있다[7][8]. 하지만, 본 논문에서 다루려는 네트워크 트래픽에 대한 은닉채널 형성 기법은 ICMP 프로토콜을 이용한 Daemon9의 [9]와 같은 연구, TCP 및 IP 헤더를 이용한 Rowland의 [10]과 같은 연구, Brinkhoff의 HTTP 프로토콜을 이용한 연구[11], 타임스탬프 메시지를 이용한 John Giffin의 [12]와 같은 연구 그리고 Christopher Abad의 [13]와 같은 IP 체크섬을 이용한 연구 등이 이루어지고 있다. 또한 단지 이론 연구뿐만이 아니라 [9-15]와 같이 TCP/IP 프로토콜에서 은닉 채널을 형성할 수 있는 도구들이 개발되고 있다. 하지만 상대적으로 은닉채널 공격기법의 연구 외에 탐지에 관한 연구[16][17]는 미미한 실정이다. 또한 최근에는 [18][19]와 같이 은닉 채널의 수학적 모델 분석 및 생성에 관한 연구도 이루어지고 있다.

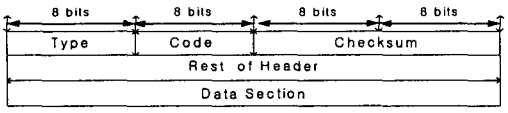
3. 은닉채널 분석

본 논문에서는 기존의 은닉채널 생성 기법들이 주 대상으로 삼았던 화상, 음성, 동영상 등의 멀티미디어 데이터에 대한 은닉채널 생성이 아닌 일반적인 TCP/IP 네트워크 환경의 네트워크 트래픽을 대상으로 하여 생성 가능한 은닉채널 기법에 대하여 분석하였다. 이러한 은닉채널 형성 기법의 분석은 생성된 은닉채널의 기능적 측면에 대한 분석이

아닌 은닉채널을 형성하는 대상 TCP/IP 프로토콜 각각의 특성을 이용한 은닉채널 생성기법에 초점을 맞추었다.

3.1 ICMP 프로토콜

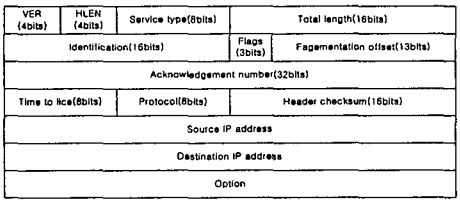
ICMP 프로토콜은 보통 다른 호스트나 게이트웨이와 연결된 네트웍에 문제가 있는지 확인하기 위하여 주로 사용된다. ICMP를 이용한 네트워크 진단 프로그램으로는 ping 프로그램이 있다. 이 프로그램을 사용하여 특정한 게이트웨이, 호스트, 라우터 등이 제대로 작동을 하고 있는지 등을 조사하며, ICMP 요청에 대한 응답시간을 검사함으로써 네트워크 상태도 어느 정도 확인 할 수 있다. 그래서 일반적으로 대부분의 네트워크는 ICMP를 사용하는 ping 패킷에 대한 접근을 허용한다. 즉, 이러한 ICMP 패킷의 네트워크 접근 가능성을 이용하여 ICMP 패킷의 페이로드 부분에 특정 정보를 포함(은닉)하여 방화벽이나 IDS와 같은 보안 장비를 보호되고 있는 네트워크에 대해서 은닉채널을 형성 할 수 있다.



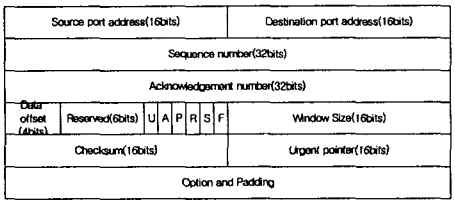
[그림 2] ICMP 헤더 구조

ICMP 은닉채널 패킷은 기본적으로 IP 페이로드를 이용해서 보내어지며, IP 헤더 포맷의 9번째 필드(프로토콜 타입)가 ICMP를 나타내는 1로 설정되어 있다. ICMP 페이로드에 특정 데이터를 삽입하여 위장이 가능한 이유는 ICMP 페이로드 부분이 가변적인 크기를 가지며 이때 ICMP 페이로드의 값은 ICMP 프로토콜을 생성하는 운영체제에 따라 다르게 설정 되기 때문이다. 또한 정상적인 ICMP 패킷의 경우 이러한 ICMP 페이로드에는 의미 없는 값들이 채워지거나 아니면 NULL 상태를 유지한다. 그러므로 이러한 ICMP 페이로드를 관찰한다 할지라도 그 의미를 파악하는 것은 쉽지 않다. 이러한 ICMP의 특성을 이용한 은닉채널 생성 도구로는 daemon9와 alhambra가 개발한 Loki, edi와 teso의 ICMP tunneling tool 그리고 CodeZero team에서 개발한 ICMP backdoor등이 있다.

3.2 IP 프로토콜과 TCP 프로토콜



[그림 3] IP 헤더 구조



[그림 4] TCP 헤더 구조

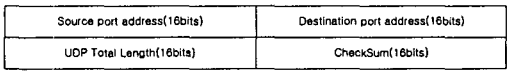
기존의 많은 연구를 통해서 TCP와 IP 프로토콜의 헤더에는 은밀한 방식으로 원격지에 있는 호스트에게 정보를 저장하거나 전송할 수 있는 많은 필드들을 가지고 있다는 것이 알려져 있다. 특히 그림 3, 4의 TCP, IP 헤더를 살펴보면, 각 헤더 내에는 *Option* 필드와 같이 프로토콜의 다양한 기능 설정을 위해서 사용될 뿐 통신과정에는 사용되지 않거나 또는 송신자의 필요로 인해서만 설정되는 필드들과 ID, SEQ 등 통신 과정에 필수적으로 사용되는 필드들로 크게 나누어 은닉채널을 형성 할 수 있음을 알 수 있다. 하지만 이렇게 데이터를 은닉하여 전송할 수 있는 공간들이 있을지라도, 전송과정에 있어서 보다 필수적인 필드에 데이터를 포함시키는 것이 은닉채널을 이용한 공격 성공률 및 탐지의 복잡성을 높일 수 있으며, 또한 이러한 전송과정에서 필수적으로 사용되는 필드들은 일반적인 TCP/IP 옵션 필드들이 패킷 필터링이나 쪼개고 재조립하는 과정에서 때때로 변화되거나 노출될 수 있다는 문제점을 가진 것에 비해 전송 도중의 변화 및 노출 가능성을 가지지 않는다는 장점을 지니고 있다.

본 장에서는 TCP, IP 헤더의 여러 필드 중에서도 IP 헤더의 ID 필드와 TCP 헤더의 SEQ 필드를 이용한 은닉채널을 생성 기법에 대해서 분석하였다. 위의 이러한 필드를 이용한 은닉채널 형성기법은 [10]에 나타나있으며, IP 헤더의 ID 필드의 경우 ID 필드를 임의의 숫자로 생성하여 특정 ASCII 값의 배가 되도록 인코딩하는 방법을 사용한다. 이러한 방법은 원격의 호스트에게 단순히 ID 필드를 읽는 것만으로 쉽게 특정 정보를 전달할 수 있게 해준다. 즉, ID 필드의 경우 'H' 값을 은닉하기 위해서는 'H'의 ASCII 값인 72를 공격 이전에 일반적인 패킷에 포함되어 있는 ID 값들의 범주와 비슷한 숫자를 생성할 수 있도록 임의의 숫자 256배를 하여 계산한 값인 18432(72*256)를 ID 필드로 생성하는 것이다. 이후 이러한 패킷을 특정 포트로 수신하는 은닉채널 서버를 구성하고, 은닉채널 서버는 특정 포트로 수신된 패킷의 ID 필드 값을 256으로 나누어 원하는 데이터를 일반적인 TCP/IP 헤더의 ID 필드를 이용하여 얻을 수 있게 되는 것이다.

TCP 헤더의 SEQ 필드 역시 ID 필드의 은닉화와 같은 방법이나 SEQ 필드(32bytes)에 올 수 있는 값의 범위는 ID 필드(16bytes)의 값보다 훨씬 크기 때문에 'H'의 경우 72*256*65536의 값으로 ASCII 값을 생성한다. 이렇게 특정 값으로 ASCII 값을 인코딩하는 것은 앞서 설명한 바와 같이 일반적으로 TCP/IP를 이용한 통신과정에서 쓰이는 패킷들이 포함하는 ID 또는 SEQ 필드 값과 유사하게 만들기 위한 것이다.

하지만 이렇게 조작된 ID, SEQ 필드를 가지고 있는 *TCP/IP* 헤더는 정상적인 TCP/IP 패킷의 헤더와는 다음과 같은 차이점을 가진다. 먼저, 조작된 ID, SEQ 필드의 값이 정상적인 패킷의 ID, SEQ 필드 값이 가지는 값과는 비슷할지라도 많은 패킷들을 패턴화 시킬 경우 일반적인 패킷들과는 상이한 패턴을 가지게 된다. 또한 각 패킷은 TCP 연결 시도와 같은 형태로 은닉 패킷을 전달하기 위하여 syn 플래그와 같이 특정 제어 플래그가 설정되어 있거나, IP flagment 필드 그리고 offset 설정 필드에 있어 일반적인 TCP/IP 패킷과는 다른 점을 가지게 된다. 비록 이러한 차이점이 있다고 할지라도 IDS의 시그너쳐 또는 패킷 트래픽의 관찰자의 직관만으로는 구분하는 것이 어려운 것이 현실이다.

3.3 UDP + DNS 프로토콜



[그림 5] UDP 헤더 포맷

UDP 프로토콜은 통신과정에서의 효율을 중점을 둔 프로토콜로서 TCP 프로토콜에서 제공하는 것과 같은 다양한 전송관련 기능을 제공하지 않는다. 그림 5에 나타나듯이 UDP 헤더 포맷은 단지 4가지의 요소를 가지는 단순한 구조을 가지고 있으며, 따라서 IP나 TCP 헤더와 달리 통신과정에서 필수적인 헤더 필드를 통해 데이터를 은닉화 시키는 것이 쉽지 않다. 하지만, UDP 프로토콜은 네트워크 환경에서 반드시 사용해야 하는 DNS 서비스에 기반을 제공한다는 특징을 가지고 있으며 또한 DNS 서비스 중에서도 DNS 질의/응답은 매우 일반적인 트래픽으로서 어떤 보안 솔루션일지라도 패킷의 흐름을 허용하는 것이 일반적이다. 즉, DNS 서비스는 내부적으로 UDP 프로토콜을 통하여 서비스를 제공하게 되고, 공격자는 이러한 점에 착안하여 DNS 질의/응답 메시지를 은닉채널을 생성하는 바탕으로 사용할 수 있으며, 이렇게 생성된 은닉채널을 통해 원격 서버에서 쉘을 실행시켜 시스템 정보를 얻어 오거나 미리 약속된 상대 시스템의 동조자로부터 특정 정보를 얻어 올 수 있다. 이러한 *UDP* 기반의 *DNS* 은닉채널을 생성하는 방법을 UDP 쉘 또는 DNS 터널링(DNS Tunneling) 기법이라고 일컬으며, 실제 예로서는 Fryxar가 만든 tunnelshell, Oskar Pearson가 만든 DNS Tunnel 그리고 THC의 van Hauser에 의해 만들어진 Daemonshell 등의 공개 도구가 있다.

이러한 은닉채널의 형성이 가능한 이유는 앞의 설명처럼 네트워크

환경에 있어 UDP 포트 번호 53번을 사용하는 DNS 서비스의 경우 일반적으로 방화벽과 같은 보안 솔루션에 의해 필터링 되지 않기 때문이며, 그러므로 DNS 질의/응답 메시지를 사용하는 은닉채널의 경우 주의 깊게 메시지의 내용을 관찰하지 않는 한 그 탐지가 어려우며, DNS 질의/응답 메시지를 통한 내부 데이터의 유출을 막는 것은 어렵다.

3.4 TCP + HTTP 프로토콜

현재의 인터넷과 거의 동의어로 사용되는 웹서비스는 HTTP라는 프로토콜을 기반으로 동작한다. 이러한 HTTP를 사용하는 웹서비스는 인터넷 트래픽의 거의 대부분을 차지하는 것은 물론이고 어떤 네트워크 환경에서도 반드시 서비스되어지는 것이 현실이다. 따라서, 이러한 HTTP 프로토콜을 이용한 은닉채널 형성 기법은 TCP/IP 트래픽을 이용한 은닉채널 형성 방법 중 가장 널리 사용되는 방법 중의 하나이며 다양한 공격 도구들이 나와있다. 또한 이 HTTP 프로토콜은 TCP 서비스를 기반으로 하기 때문에 HTTP를 이용한 은닉채널의 형성은 항상 TCP 전송 메커니즘을 염두해 두어야 한다. HTTP 프로토콜을 이용하여 은닉채널을 형성하는 방법은 HTTP가 지원하는 GET, POST, HEAD 메소드 요청에 데이터를 은닉화하여 일반 HTTP 트래픽과 구분하게 어렵게 만드는 방식 또는 공격자가 공격 대상으로 여기는 네트워크 내부의 주소를 가지고 나오는 HTTP 트래픽에 특정 정보를 삽입하여 외부로 정보를 유출하는 방법 등 다양하게 존재한다. 특히 HTTP를 이용한 은닉채널은 HTTP 프락시 서버를 이용하여 내부 네트워크에 존재하는 특정 서버에 접근을 허용해주기도 한다. 이러한 TCP 기반의 HTTP 은닉채널을 생성하는 방법을 HTTP 쉘(HTTP Shell), HTTP 터널링(HTTP Tunneling), web 터널링(Web Tunneling) 기법이라고 일컬으며, 실제 예로서는 THC의 van Hauser에 의해 만들어진 Rwwwshell, Brinkhoff에 의해 제작된 GNU httptunnel, Jos Visser의 proxytunnel 그리고 Alex Dyatlov에 의한 web shell 등의 공개 도구가 있다.

이러한 HTTP를 이용한 은닉채널의 형성이 가능한 이유는 앞의 설명처럼 네트워크 환경에 있어 HTTP를 이용하는 웹서비스는 필수적인 요소이고, TCP 포트번호 80을 이용하는 HTTP 서비스의 경우 일반적으로 방화벽과 같은 보안 솔루션에 의해 필터링 되지 않기 때문이다. 하지만, 이러한 HTTP 은닉채널의 공격이 가능할지라도 HTTP 트래픽을 분석하는 것은 HTTP 트래픽이 네트워크 트래픽 양에 차지하는 비율을 고려할 때 쉽지 않은 일이다. 특히 내부 네트워크로부터 나오는 HTTP 트래픽의 경우 은닉채널을 생성하였다면 그 탐지는 더욱 어렵다.

4. 향후 연구 방향

은닉채널에 관한 연구는 현재 주로 동영상에 대한 정보 은닉 기법에 대해서 주로 이루어지고 있지만, 인터넷 환경의 표준 프로토콜로서 불릴 수 있는 TCP/IP 네트워크 트래픽에 대한 은닉 채널 형성 기법 역시 현재 활발히 연구 되고 있는 것을 알 수 있었다. 하지만, 은닉채널 형성을 통한 공격 기법 자체에 대한 연구는 많은 진척을 보이고 있지만 실제적으로 이런 은닉채널 형성 공격이 이루지는것에 대한 대응 방안에 관한 연구는 매우 미비하다. 하지만 일반적인 트래픽 분석등과 같은 방안을 통해서는 일반 네트워크 트래픽과 그 차이점을 발견하기 어려움 은닉채널 형성기법을 이용한 은닉채널을 탐지하는 것이 거의 불가능하다. 따라서 향후에는 은닉채널공격에 대한 SVM, 신경망등과 같은 학습기법의 적용 연구가 필요할 것이다.

5. 결론

은닉채널이란 매개체를 이용하여 특정 정보를 은닉해주는 채널로 쉽게 생각할 수 있다. 이러한 은닉채널에 대한 위협성은 보통 멀티미디어 데이터에 대한 스테가노그래피 형태로 알려져 왔으나, 현재에는 네트워크 트래픽을 이용한 공격 방안 역시 그 위협성이 대두되고 있으며, 이러한 네트워크 트래픽을 이용한 은닉채널 공격은 쉽게 파악될 수 있는 시스템 및 네트워크 취약성을 이용한 해킹 공격보다 훨씬 큰 잠재적 위협성을 내포하고 있다.

본 논문에서는 인터넷 환경의 사실상 표준인 TCP/IP에 초점을 맞추어 각 프로토콜 별로 생성될 수 있는 것으로 알려진 은닉채널 기법을 분석하였다. 현재는 이러한 분석을 바탕으로 신경망 및 기계학습 기법을 이용한 네트워크 트래픽 은닉채널 탐지에 관한 연구가 수행 중이다.

5. 참고문헌

[1] Department of defence trusted computer system evaluation criteria, Tech. Rep. DOD 5200.28-ST, Department of Defence, December 1985. Supersedes CSC-STD-001-83.

[2] K. Ahsan and D. Kundur, "Practical Data Hiding in TCP/IP" Proc. Workshop on Multimedia Security at ACM Multimedia '02, 7 pages, French Riviera, December 2002.

[3] B. W. Lampson, A note on the confinment problem, in Proc. of the Communications of the ACM, no. 16:10, pp. 613 615, October 1973.

[4] P.A. Porras and R.A. Kemmerer. Analyzing covert storage channels. In Proc. 1991 Symposium on Research in Security and Privacy, pages 36--51, Oakland, CA, May 1991. IEEE Computer Society.

[5] J.C. Wray. An analysis of covert timing channels. In Proc. 1991, Symposium on Research in Security and Privacy, pages 2--7, Oakland, CA, May 1991. IEEE Computer Society.

[6] J. McHugh, Covert Channel Analysis, Technical Memorundum 5540:080A, Naval Research Laboratory, Washington D.C., 1995. A Chapter of the Handbook for the Computer Security Certification of Trusted Systems.

[7] Neil F. Johnson et al, Information Hiding: Steganography and Watermarking - Attacks and Countermeasures, Kluwer Academic Publishers, 2000.

[8] Fabien A. P. Petitcolas, editor. Information hiding. Proceedings of the 5th international workshop on information hiding, vol. 2578 of Lecture Notes in Computer Science, Noordwijkerhout, The Netherlands, 7.9 October 2002.

[9] daemon9 and alhambra. "Project Loki: ICMP Tunnelling." Phrack Magazine, Volume Seven, Issue 49, File 6 of 16, August 1996. http://phrack.infonexus.com/search.phtml?view&article=p49-6

[10] C. H. Rowland, Covert channels in the TCP/IP protocol suite, Tech. Rep. 5, First Monday, Peer Reviewed Journal on the Internet, July 1997. URL:http://www.psionic.com/papers/covert/covert.tcp.txt

[11] John Giffin, Covert Messaging Through TCP Timestamps, PET2002

[12] Christopher Abad, IP Checksum covert channels and selected hash collision, www.securityfocus.com, 2001

[13] Oskar Pearson, "DNS Tunnel - through bastion hosts", ICON, http://www.icon.co.za/~wosp/wosp.dns-tunnel.tar.gz

[14] van Hauser., rwwwshell, http://www.thc.org/releases/rwwwshell-2.0.pl.gz

[15] Alex Dyatlov, web shell, http://www.entreelibre.com/simsim/wsh/

[16] Gina Fisk,Eliminating Steganography in Internet Traffic with Active Wardens, F.A.P. Petitcolas (Ed.): IH 2002, LNCS 2578, pp. 18 35, 2003. Springer- Berlin Heidelberg 2003

[17] Sohn TaeShik, Seo Jung-Taek, Moon Jong-Sub, "A Study on the Covert Channel Detection of TCP/IP Header using Support Vector Machine", ICICS 2003, LNCS 2836, Springer-Verlag Berlin Heidelberg 2003

[18] Alexander Grusho, "Mathematical Models of the Covert Channels", V.I. Gorodetski et al. MMM-ACNS 2001, LNCS 2052, pp. 15-20, 2001. Springer-Verlag Berlin Heidelberg 2001

[19] Alexandre Grusho and ElenaTimonina, "Construction of the covert channels", V.I. Gorodetski et al. (Eds.): MMM-ACNS 2003, LNCS 2776, pp.428-431, 2003. Springer-Verlag Berlin Heidelberg 2001