情 報 保 護 學 會 誌
第 16 卷 第 1 號, 2006. 2

DoI(Denial of Information) 공격 동향과 대응 프레임워크 분석

김 국 한*, 최 병 철*, 유 종 호*, 서 동 일*

요 약

현대의 인터넷 환경에서는 다양한 서비스 채널을 통해 정보의 유통이 활발히 이루어지고 있다. 이러한 환경에서는 기존의 정보보호의 한계를 이용하는, 특히 사회 공학적 공격 기법을 활용하는 DoI(Denial of Information, 정보거부) 공격과 같은 사이버공격으로 인해 중요한 보안 문제를 유발 할 수 있다. DoI 공격은 악의적인 공격자가 유용한 정보임을 가장하여 의도적으로 악성정보를 포함하여 유통함으로서, 네트워크 사용자가 원하는 정보를 찾아서 자기 것으로 만드는데 필요한 다양한 가용 자원을 소모하도록 하는 공격이다. 본고에서는 현재 만연하는 DoI 공격의 형태 및 상황을 알아보고, DoI 공격을 대응하기 위한 프레임워크는 어떤 것이 있는지 살펴본다.

Ⅰ. 서 론

네트워크는 사용 환경 및 시대적 요구에 따라 꾸준하게 진화한다. 현재 우리나라의 차세대 네트워크는 광대역통합망(BcN) 형태로 진행 중이다. Broadband Convergence Network(BcN)은 음성·데이터 통합, 유·무선 통합, 통신·방송 융합 등을 통하여 다양한 서비스를 하나의 네트워크로 제공하는 것이다[1]. 또한 현재 인터넷의 유통 정보량은 170TB/day (17xLOC)로 인스턴트 메신저는 750GB/day or 274TB/yr, E-mail은 400,000TB/yr, 비디오 동영상 및 MP3 파일 등이 P2P 파일 공유 프로그램을 통한 전파가 급증하고 있다[2]. 이러한 네트워크 진화 및 정보량의 유통 증가 더불어 가장 중요하게 보장되어야 하는 기술이 바로 정보보호 기술이다.

DoI(Deinal of Information) 공격은 악의적인 공격자가 일반 사용자들이 선호하는 유용한 정보를 가장, 혹은 악의적인 불법 정포를 포함시켜 유포함으로 정보에 대한 거부현상을 일으키도록 하여 종국에는 서비스에 대한 불신을 유도하는 공격이다. 이런 공격은 일반적으로 P2P, IM(Instant Messenger), E-Mail 등과 같이 정보를 공유·유통시키는 네트워크 서비스를 사이버공격의 매개체로 이용한다. 여기에는 네트워크 인프라의 발전과 함께 급격하게 사용자 수가 증가함에 따라 사이버공격 시간과 비용을 극소화 시키며 전파 속도를 극대화 할 수 있다는 장점이 있기 때문이다. 그리고 이전에는 해커들이 자신의 실력을 과시하기 위한 수단으로 명성을 얻는 것으로 만족했지만, 요즘은 금전적인 목적을 가진 공격이 증가하고 있다[3].

따라서 각종 사이버공격에 의한 네트워크 서비스 가용성 제한, 악성 정보의 범람으로 정보의 신뢰성 상실에 의한 간접적인 네트워크 기능 약화 그리고 마지막으로 현실적으로 나타나는 금전 피해를 막기 위해서는 효과적인 보안 대응책이 요구된다.

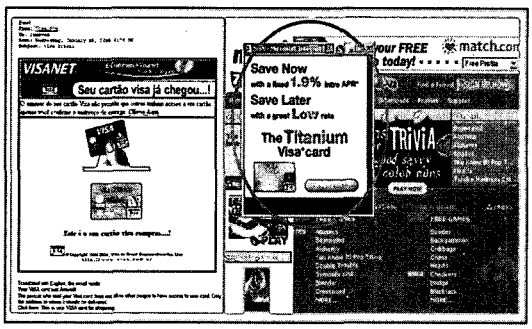
본고에서는 DoI 공격에 관한 여러 가지 동향을 알아보고, DoI 공격을 대응하기 위해 조지아공대에서 제시한 분류(Taxonomy)와 프레임워크를 살펴본다.

Ⅱ. DoI(Denial of Information) 공격

DoI 즉, 정보거부 공격은 QoS/DoS의 개념이 확장 된 것이다. QoS(Quality of Service)는 종단간의 성능 향상이 주요 이슈로서 관련 metrics는 네트워크 대역폭(network bandwidth)과 전송지연(latency)이다. 그리고 DoS(Denial of Service)는 특정 네트워크 노드에 과부하를 유도하여 시스템 가용 자원(processing, memory, bandwidth 등)을 소진함으로서 정상적인 사용자의 QoS 가용성을

* 한국전자통신연구원 정보보호연구단 네트워크보안구조연구팀 ({kimkook, corea, ryubell, bluesea}@etri.re.kr)

위협하는 악의적인 공격이다. 이와 유사한 개념으로 선의의 사용자들이 원하는 유용한 정보 - QoI (Quality of Information) - 유통을 방해하는 공격이 DoI라고 할 수 있다. 그러나 DoS를 포함하는 DoI 공격이 조금 더 큰 개념으로서 사용자의 컴퓨터를 통해 의도적으로 사용자의 자원들을(time, cognitive processing, perceptual capabilities, memory 등) 소진하도록 하는 모든 공격을 의미한다[4].



〔그림 1〕 DoI 공격 예 (Phishing Scam)

2.1 공격 목적

DoI 공격의 목적은 여러 가지로 볼 수 있다. 우선 정보거부(Denial of Information)라는 의미상 목적을 보면, 인터넷에 대량의 불법 및 악성 정보 유통을 통해 정보로서의 효용성을 떨어트림으로서 선의의 사용자로 하여금 정보에 대한 거부감을 유도하여 네트워크 서비스에 대한 불신을 초래하는 것이라고 볼 수 있다. 즉 DoS가 네트워크 서비스 제공자 입장에서 서비스를 하지 못하게 하는 것이라면, DoI는 정보 요구자가 유용한 정보를 얻지 못하도록 하는 것을 의미한다. 여기에는 단순히 검색엔진에서 적합하지 않은 정보를 우선순위로 올려서 인지(cognitive) 능력에 혼선을 주거나, 스팸메일을 통해 사용자의 처리시간(time)을 소모하게 만든 것도 하나의 목적이 될 수 있다.

최근에 발생하는 DoI 공격의 주요 목적은 사용자가 원하는 유용한 정보(signal) 속에 악성정보(noise)를 집어넣음으로써 개인 및 기업의 민감한 정보를 유출하고 이를 이용하여 금전적인 이득을 취하는 것이다.

2.2 공격 방법

DoI 공격 방법은 크게 Mass/Massive 공격과 Targeted /Gradual 공격으로 구분 할 수 있다.

"웜/바이러스, mail bomb"과 같은 형태로 불특정 다수에게 위조된 정보를 대량으로 살포하는 mass 공격은 인터넷에서 가장 일반적인 형태이다. 이 공격의 목적은 가능한 많은 PC와 서버를 감염시키는 것이다. 일반적으로 이 공격은 IT 서비스 채널의 취약점이나 사람의 취약점(사회공학적인 방법을 이용하여)을 이용한다. Signature 기반 탐지/방지 기술이 mass 공격에 효과적으로 대응하기 때문에, mass 공격이 일반적이지만 실제 피해를 주는 경우는 상대적으로 낮다.

반면 악성코드를 내포한 불법 정보를 목표물을 향해 은밀하게 유통하는 Targeted 공격은 특정 회사 혹은 특정인에게 영향을 주기 위한 목적을 가진 공격으로 꾸준히 증가하는 추세이다. Targeted 공격은 다음과 같은 3가지 주요 목적을 가진다.

- Denial of Service: 사업을 방해
- Theft of Service: 상용 제품/서비스 무상 획득
- Information compromising: 기업 중요 정보 절취, 파괴, 변형

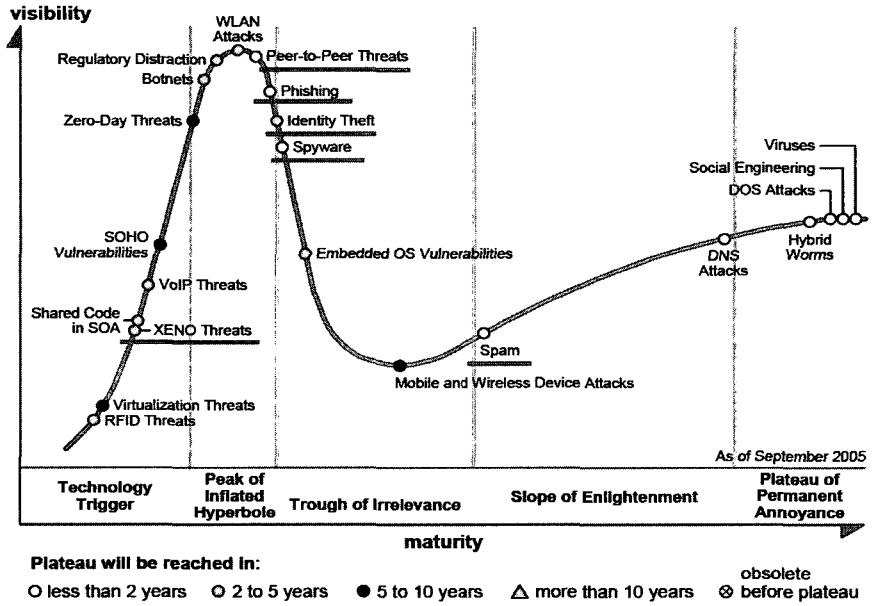
최근의 DoI 공격은 갈취(extortion), 훔친 정보에 대한 대가(ransom) 요구, 훔친 신원 정보를 범죄 그룹에 판매(selling)와 같이 금전 취득이 주요 동기이다.

네트워크상에서 발생하는 공격 유형을 보면 10% 정도가 목표를 정해두고 공격하는 Targeted 공격이고 그 외 나머지 90% 정도는 웜/바이러스와 같이 불특정 다수를 목표로 하는 공격이다. 그렇지만 공격 성공에 따른 영향은 Targeted 공격이 mass 공격보다 50~100배 정도 크다. 따라서 표적공격에 대한 대비가 필요하다[5].

2.3 공격 형태

가트너 그룹에서 발표한 설문조사 보고서[6]에 따르면 2005년 사이버위협에 관한 분석에서, 현재 주로 이루어지는 DoI 공격 형태인 스팸메일, 피싱(Phishing), 파밍(Pharming) XENO(eXtended Enterprise Network Overseas) 공격 등이 그림 2에서와 같이 발생기와 성숙기 부분에 포진하고 있다.

최근 가장 빈번하게 일어나는 공격이 스팸 메일을 통한 피싱(Phishing)이다. 피싱은 주로 금융권 회사임을 가장하여 불특정 다수에게 사용자가 유리한 조건을 담은 메일을 전송하여 개인정보를 요구하거나, 잘 알려진 금융 사이트로 오인하도록 만든 위조 사이트로 유인하여 개인의 신용정보 및 금융정보를 유출하고 금전적인 피해를 입히는 공격이다. 최근 보고서[7]에 따르면 피싱 공격으로 여겨지는 e-mail의 수신이 증가



〔그림 2〕 Hype-cycle for Cyberthreats 2005

함에 따라, 첨부를 클릭하여 악성 코드가 사용자 시스템에 설치되어 정보를 유출하거나, 메일을 확인함과 동시에 해당 유해 사이트로 이동하여 자신의 신용정보를 노출해서 금전적인 피해도 증가하고 있음을 설문조사 결과로 알 수 있었다.

또한 피싱과 유사한 파밍은 합법적으로 소유하고 있던 사용자의 도메인을 탈취하거나 도메인네임시스템(DNS) 이름을 속여 사용자들이 진짜 사이트로 오인하도록 유도, 개인정보를 훔치는 새로운 수법이다[8]. 파밍의 사례를 보면 미국의 Panix(ISP업체) 도메인이 알려지지 않은 사람의 요청에 의해서 탈취된 사건, 독일 eBay 사이트가 19세 청년의 사이트 변경 신청에 의한 사이트 탈취 사건, 그리고 도메인 해킹으로 추정되는 사건으로 도백개의 도메인 서비스가 중단되고 국내'.tv' 151개 사이트 소유자가 변경되는 사건이 발생하였다. 전문가의 분석[9]에 따르면 DNS 서버 10% 정도가 파밍 공격에 무방비 상태라고 분석하고 있다.

피싱과 파밍의 결정적인 차이점은 피싱은 유명사이트와 유사하게 만든 사이트로 유인하고, 파밍은 실제 사이트 주소를 탈취하거나 합법적인 사이트 주소를 이용한다는 것이다.

국제 피싱 방지 실무그룹인 APWG(Anti-Phishing Working Group)의 2005년 11월 보고에 따르면 통합·지능형 피싱 공격이 금융권에 집중되고 있으며, 2005년 11월에 동작 중인 피싱 사이트는 총 4630개이며 평균 5.5일 작동하지만 최근에는 31일 동안 작동하는 경우도 있다고 보고하고 있다[10].

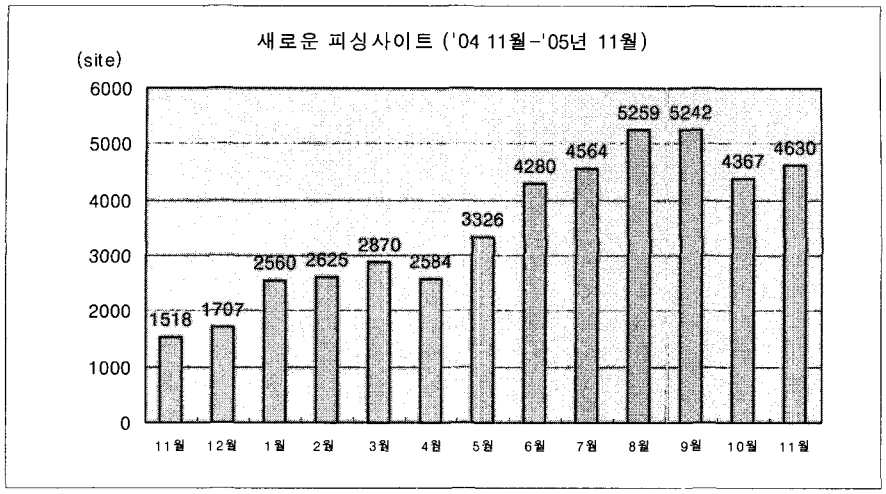
그리고 P2P(Peer-to-Peer) Overlay 네트워크와 같은 back-end processing 서비스를 이용하여 개인이나 기업의 중요 정보를 유출하는 목적을 가진 공격 형태가 있다. 특히 P2P와 IM(Instant Messenger)의 경우에는 새로운 음악/미디어 파일을 P2P로 구하는 사람이존재하고 있는 이상, 악성 코드를 확산하는 매체로서 꾸준히 이용될 것이며, 최근에는 국내 OO은행 지점장이 작성한 1040명의 상세한 개인정보(인적사항, 거래, 대출, 신용등급 등)가 P2P를 통해 유출되는 사고가 발생하였다[11]

2.4 DoI 공격 대응 방법

현재 DoI 공격은 여러 가지 형태로 성행하고 있지만 실질적으로 여기에 대처하는 노력은 산발적으로 이루어지고 있다. 따라서 DoI 공격에 대한 대응방법으로 아래와 같은 사항이 요구된다.

- QoI(Quality of Information) 보증(assurance)
- SCM(Secure Content Management)
- DoI 공격 Taxonomy & Framework

DoI 공격을 대응하기 위해서는 전통적으로 정보보호에서 다루었던 기밀성(confidentiality), 무결성



[그림 3] 최근 1년간 피싱 사이트 신설동향

(integrity), 정보의 가용성(availability) 등의 개념에서 더욱 확장된 보안 요소인 QoI(Quality of Information) 보증(assurance)이 포함되어야한다[12]. 즉, 처음부터 DoI 공격자가 유용한 정보임을 가장하여 유통시킨다면 이는 정보보호의 기본적인 요소인 무결성에 위배되지 않는다. 다시 말하면 그 정보가 유용(signal)한지 아니면 악성(noise)인지는 보장이 되지 않는다는 것이다.

일관성(consistency), 적시성(timeliness), 신뢰성(reliability, trustworthiness) 그리고 정보의 밀도/풍부함(density/richness)와 같은 척도들(metrics)로서 서비스 품질(QoS)을 검증하는 것과 마찬가지로 정보의 품질 (QoI)을 검증 할 수 있는 여러 가지 척도들이 정의 되어야하고, 조지아공대 Mustaque Ahamad 교수는 정보의 규칙성(regularity)과 품질 신뢰(quality trust)를 제시하고 있다[12].

또 하나 주목해야할 사항은 최근 SCM(Secure Content Management) 시장이 급부상 중이라는 것이다. SCM은 정책기반 컨텐츠 보안 솔루션으로 메시지와 웹 트래픽 통한 위협을 안전하게(secure), 탐지하고(monitor), 필터링(filter)하여 차단(block)하도록 디자인된 보안도구로서 inbound 위협 뿐 아니라 outbound로 나가는 중요한 정보, 고객 기록, 지적 재산권 등이 유출되는 것을 차단한다.

SCM 시장의 규모는 2004년 $45억(4.5조) 규모였고 이는 2003년의 $35억(3.5조)보다 28% 정도 급증했다. 그리고 2009년에는 $105억(10.5조)으로 예측되며 성장률(2004-2009 CAGR)은 18.7%이다[13].

마지막으로 다음 장의 DoI 공격 분류 및 프레임워크로서 다양한 시나리오를 가지고 검증이 필요하다.

III. DoI 공격 분류(taxonomy) 및 프레임워크

이번 장에서는 현재 조지아공대(Georgia Institute of Technology) 박사과정인 Gregory Conti가 제안한 DoI 분류 및 프레임워크에 대해서 살펴본다.

그전에 한 가지 전제를 두고 분석을 진행한다. 앞에서 살펴보았던 DoI 공격 목표 중에서 이번 장에서는 유용한 정보를 원하는 사용자나 노드의 가용 자원을 소진하는 것을 목표로 하는 DoI 공격에 중심을 맞춰 분석을 진행한다.

분류와 프레임워크는 DoI 공격의 객체(object)와 행동(action)을 고려하였다. 비록 절대적인 정당성과 완벽성은 어렵지만, 2004년 초부터 2005년 초까지 12개월 동안 Slash.org에서 DoI 공격의 여러 가지 형태를 분석하였고, 결과적으로 DoI 공격의 일정 패턴을 확인 할 수 있었다. 새로운 형태의 DoI 공격은 여기서 제시한 분류와 프레임워크를 더욱 개량하는데 도움이 되었고 반복적으로 검증할 수 있었다. 우선 프레임워크를 이루는 6가지 주요 개념에 대해 알아본다[4].

- Node: 정보를 만들거나 소비하는 시스템으로 Processing, I/O, Storage와 같은 가용 자원이 한정적이다. 대부분의 경우 통신 채널을 통해 노드간의 연결을 한다.

- Communication channel: 정보를 송신하는 노드로부터 수신하는 노드로 메시지를 전달하는 통로로서 전송 대역폭의 한계를 가지고 있다.
- Information object: 데이터영역 안의 모든 개별적으로 저장 가능한 객체로서 모든 객체는 유용한 정보(signal)와 유해정보(noise)로 나뉠 수 있다.
- Information universe: 모든 node, information object와 communication channel 셋(set)
- Human: 노드를 사용하는 사용자로 보고 듣는 input과 운동수단(motor skill)과 말하는 output으로 상호작용을 한다. 이때 인식처리(cognitive processing), 지각력(perceptual capability), 그리고 메모리(memory)등 제한적인 가용 자원을 가지고 있다.
- DoI: 정보 노드나 사람이 원하는 정보 수집 능력을 감소시켜 속이거나 가용 자원을 낭비하도록 하는 것

여기서 제안한 프레임워크의 주요 객체(object)는 위에서 분류한 4가지- 노드(information node), 통신채널(communication channel), 사람(human) 그리고 정보 객체(information object)-이다. 그리고 행동(action)은 생성(production), 소비(consumption), 공격(attack) 그리고 방어(defense)로 분류된다.

3.1 행동(action)의 분류

행동은 정보 생성 및 소비 뿐 아니라 공격이나 방어의 형태로 나타난다. 공격의 목표물은 정보 생산자, 소비자, 통신채널 그리고 사람이나 시스템에 의해 취약점을 가지고 있는 데이터 처리 등이 될 수 있다. 여기서 각각을 개별적으로 분리해서 알아본다[4].

- **Production** - 생산자는 다른 노드에게 직접 혹은 다른 노드, 사람, 또는 센서를 통해 수집한 정보를 제공하는 정보 노드이다. 이 때 제공한 정보는 정확한 것부터 부정확한 것까지 다양하며, 정보 수신자의 보호 수단을 피하기 위한 대응책을 이용할 수도 있고, 의도적으로 악성정보를 유용한 정보처럼 포장하여 유통시킬 수도 있다. 이러한 대응책에는 수신 측의 보호 수단을 우회하기 위해 정보를 변형하는 것도 포함된다. 특히 스팸의 경우를 보면, 수신 측 필터링 메커니즘을 피해 통과하려고 제목을 교묘히 조작한다.
- **Consumption** - 소비자(수신자)는 검색 엔진의 질의를 통해 생산자로부터 정보를 직접 받아들이거나, 내가 원하든 원하지 않던 보내진 메일을 수신하는 정보 노드이다. 일반적으로 정보 소비자는 원하지 않는 정보(noise)를 제거하고 원하는 정보(signal)만을 얻기를 원한다. 그러나 대부분의 경우 점점 많은 noise가 자신들의 방어 수단을 통과 할수록 DoI 공격의 성공 가능성은 더욱 커진다.
- **Attack** - 공격은 의도적이든 아니든 사람이 받은 정보의 질을 저하하려고 한다. 이것은 S/N 비율이 낮을 때 명확하게 나타난다. 표 1은 DoI 공격의 4가지 주요 시나리오이다.

이상적인 웹 검색은 믿을만한 검색 엔진을 통해 얻은 결과에서 noise는 작고 signal이 많은 상황이다(시나리오 2). 악의적인 사이트에서는 결과가 반대이다(시나리오 3). 만일 사용자가 부적절하게 입력하여 검색한다면 최소한의 정보만을 얻거나(시나리오 1) 믿을만한 사이트이지만 전혀 다른 정보를 얻을 수 있다(시나리오 3). 공격자는 정보 검색자가 원하는 정보를 필요한 시간에 못 받도록 방해하거나 정상적인 정보처럼 보이는 noise를 전송함으로서 DoI 공격을 성공한다. 이런 현상은 인간의 정보처리 능력에 부하가 걸리거나, 노드의 하드웨어나 네트워크상에 문제가 생기는(Denial of Service) 경우이다(시나리오 4). 공격자나 방어자 모두 자신들의 성공 가능성을 높이기 위해 나름대로의 대비책을 사용한다. DoI 공격의 성공 여부는 공격에 따른 목표물의 의사결정(decision- making) 능력에 어떤 영향을 미치는 지가 중요한 척도이다. 바꿔 말하면, 목표물에서 변화가 얼마나 있느냐를 의미한다(표 2 참조).

〔표 1〕 DoI 공격 시나리오

	Signal (S)	Noise (N)	S/N	Impact
시나리오1	low	low	parity	- 정보를 찾는 최소한의 능력
시나리오2	high	low	good	- 정보를 찾는 훌륭한 능력
시나리오3	low	high	bad	- DoI
시나리오4	very high	very high	parity	- DoI 혹은 DoS (처리 능력, I/O, 저장 초과 등)

〔표 2〕 목표물에 따른 DoI 공격 형태 분류(Taxonomy)

사람 (Human)	처리 (Processing)	인지 (Cognitive)	메모리 (Memory)	인지버퍼 (Perceptual Buffer)	- 마술사의 손놀림: 시력이 분별할 수 있는 것보다 빠르게 움직임
				단기간 (Short term)	- 무작위로 선별된 긴 비밀번호 선택
				장기간 (Long term)	- "친숙한" 소스로부터의 스팸메일
					- 여러 가지 비밀번호 기억하기
			인지과정 (Cognitive processing)		- 새로운 사람(newcomer)을 배제하기 위한 고급 전문용어 사용
	입력 (Input)	시각 (Vision)			- 깜빡이는 광고
		청각 (Hearing)			- 시끄러운 락 음악 재생
	출력 (Output)	언어 (Speech)			- 도청을 위해 부드럽게 말함
		운동능력 (Motor)			- 인증을 위해 키보드 탄도를 모니터링
시스템 (Machine)	처리(Processing)				- 공격자가 inbound packet을 무수히 보내 가용자원을 낭비시킴
	입력(Input)				- Distributed Denial of Service (DDoS) 공격
	출력(Output)				- 도청을 피하기 위한 암호화 출력
	저장 (Storage)	Primary storage (ROM/RAM)			- 시스템 기본 I/O(BIOS) 손실(Corrupting)
		Secondary storage (Hard deive)			- IDS(Intrusion Detection System) 로그가 넘치도록 트래픽 공격

· **Defense** - 공격과 방어는 항상 양립하는 개념으로, 공격노드와 방어노드 모두 DoI 공격 및 방어의 가능성을 높이거나 줄이기 위해 자신들의 여러 가지 대응수단을 이용한다. 방어자는 법률적(legal), 규율적인(regulatory), 윤리적(moral), 문화적(cultural), 조직적(organizational), 금전적(financial), 기술적(technological) 그리고 심지어는 폭력적인(violent) 방법(countermeasure)을 통해 자신의 정보 환경의 noise를 줄이고 signal을 높이려고 노력한다. 표 3에서 보듯이 공격자 역시 비슷한 방법을 통해 성공적인 DoI 공격 가능성을 높이기 위해 노력한다.

3.2 기술적인 방어(defense)의 분류

앞서 살펴보았듯이 공격자와 방어자는 각자의 정보환경이 자신이 원하는 시나리오대로 진행되도록 노력한다. 이를 위해서는 표 3에서 살펴보았듯 여러 가지 제도적·사회적 방법을 통해 DoI 공격 및 방어를 성공적으로 수행하기를 원한다. 이러한 방법 중에서 표 4와 같이 기술적인 방법에 초점을 맞춰 세부적으로 살펴보고자 하며, 각각은 S/N 비율을 높이기 위한 기술이다[4].

· Filtering: 필터링은 자신이 원하는 정보환경을 만들기 위해 널리 사용되는 방법이다. 최근에 필터링에서 사용하는 방법을 보면 키워드, 베이지안(Bayesian)[1]식 및 협업 필터링 등이 있다. 그리고 정보의 질을 향상시키기 위해 사람이 정보를 확인 후 데이터베이스에 저장하는 human-in-the-loop 시스템이 있다.

· Resource-consumption: 잠재적인 공격자들에게 한정적인 자원(money, processing, time)을 지불하게 함으로서 공격 효율성을 저하시키는 방어수단이다. 적응형-자동화 시스템은 작업에 요구되는 최소한의 자원만으로 효율적인 정보를 얻을 수 있어서 다른 대응수단을 위한 자원의 여유가 생긴다.

· Meta-information: 외부에서 얻은 정보를 데이터 셋(data set)과 매치(match)를 시킨다. 정보의 질 측정과 신뢰척도(trust metric)등이 포함된다.

· Trusted computing: 정보 제공 노드의 무결성(integrity)을 보증한다. 만일 시스템이 감염되었다면 그 시스템에서 제공되는 정보는 의심스럽다.

1) 수학자였던 토마스 베이즈(Thomas Bayes)의 정리를 텍스트 분류(Text Classification)에 적용한 것으로, 특정 텍스트에서 개별 단어의 출현 빈도를 모두 기록한 뒤, 비슷한 분류의 텍스트를 계속 샘플 데이터로 추가시켜나가면서 단어들의 연관을 추적하여 임의의 텍스트가 해당 분류에 속하는지 여부를 알 수 있다는 이론이다.

〔표 3〕 DoI 공격에 대한 방어 분류(Taxonomy), by big picture

형태 (Type)	대응책 (Countermeasure)	예 (Example)
법률 (Legal)	법률	- 소규모 mp3 배포자에 대한 미국 음반협회의 소송
	새로운 법	- 뉴욕주의 no-call 데이터베이스
규정 (Regulatory)	정부규정	- 미디어 합병 승인 (US 연방 통신 위원회)
윤리 (Moral)	홍보캠페인	- 영화 저작권 침해에 대한 영화사측 캠페인
	윤리법규	- 회원에 대한 윤리법규 부과 (미주 변호사협회)
문화 (Cultural)	커뮤니티	- 그룹에서 제명
조직 (Organizational)	DoI 대응 단체	- 안티스팸 컨소시엄 설립
금전 (Financial)	DoI 운영 비용 증가	- 우편요금 인상
폭력 (Violence)	DoI 가해자에 대한 폭력	- 텔레마케팅 회사에 협박 메시지 전달
기술 (Technology)	〔표 4〕 참조	

- Data fusion: 유용한 정보를 만들고 인지(cognitive) 능력 부담을 줄이기 위해 이종의(disparate) 소스로부터 나온 정보를 통합해서 정보량을 줄인다.
- Database keys/indices: 검색 엔진에서 부적절한 키워드를 사용하여 검색결과로 상위에 위치하는 웹사이트를 금지한다.
- Source-evaluation: 양질의 정보를 제공하는 믿을만한 정보 소스인가를 확인하는 기술이다. 이 평가 기술은 도전-응답(challenge-response) 기술 또는 사용자가 시스템인지 사람인지 확인하는 테스트도 있다. 그리고 소스 익명성도 고려하는데 이것은 양면의 칼과도 같다. 익명이기에 악성 정보를 유통 시킬 수 있는 반면 오히려 익명성으로 인한 자유로운 발언으로 정보의 질을 향상 시킬 수도 있다.
- Structuring data: 개선된 데이터 구조는 관련 정보의 검색 효율성을 높일 수 있다. XML과 같은 기술은 지식을 정보에 반영하여 결과적으로 암호화를 개선시킨다.
- Restricted connectivity: 기관의 데이터 손실을 차단하거나 가능성을 줄여준다. 예를 들면 "air-gapped" 광대역네트워크(WAN)은 기관의 시스템으로만 연결을 하고 인터넷 접근은 차단하여 직접적인 데이터 손실을 줄인다.
- Translating data: 사용자의 요구를 충족하는 정보를 제공한다. XML은 변환을 도와주는 도구가 있고, 다른 예로 서로 다른 포멧과 Babel-Fish.com과 같은 언어 번역 시스템을 변환해주는 미들웨어도 있다.
- Human-computer interface: 자신의 시스템과 상호작용을 하는 효율적인 방법이다. 보다 이해하기 쉽고 효율적인 그래픽으로 정보를 제공하여 사람의 인지(cognitive) 부담을 줄여주는 정보 시각화(information visualization)가 좋은 예이다. 이로 인해 확실한 판단을 하거나 새로운 정보 발견에 많은 도움이 된다.
- Data protection: 정보의 변형이나 공격 침입 탐지 시스템을 통해 특정 소스로부터 제공된 정보의 신뢰성을 얻을 수 있다. 예를 들면 Trip-Wire 시스템은 정보시스템 파일의 변화이나 주어진 자료의 무결성(integrity)을 보호하는 공개키 기반의 암호문 사용을 탐지할 수 있다. 최신의 탐지 시스템은 "자가 치료(self healing)" 기술과 연동하여 공격으로 인한 손실을 복구한다. 또한 정보보전(preservation)을 관련 주제로 손상되거나 왜곡된 정보 보호수단이 관심을 끌고 있다. 좋은 예가 웹 페이지의 스냅 사진을 저장하는 구글(Google)이나 Internet WayBack 시스템의 웹 페이지 저장(cache)기능이다.
- Locating data: 데이터 위치선정은 사용자가 원하는 정보가 이전에는 어디 위치했었는지 같은 위치정보 뿐 아니라 처음에 정보를 찾는 것도 도와준다. 예를 들면 웹 브라우저가 제공하는 북마크나 히스토리 관리 기능이다.

3.3 DoI 공격 대응 시나리오

지금까지 앞장에서 DoI 공격의 분류(taxonomy)와 프레임워크를 알아보았다. 이를 기반으로 여기서 DoI 공격의 적절한 예인 스팸을 살펴본다[4].

스팸은 DoI 공격의 가장 일반적인 형태이다. 메일 수령인은 관심 없는 메일(noise)은 제외하고 관심 있는(signal) 내용을 담은 메일(information object)을 받기를 원한다. 스팸 발송인의 목적은 수취인이 자신의 상품, 서비스 혹은 어젠더(agenda, 문제 해결

〔표 4〕 DoI 공격에 대한 방어 분류(Taxonomy, by technological

Filtering	협업 필터링	- Slash.org
	필터링 알고리즘	- 연결 분석(Link analysis), 근사값(Proximity) 조사, 순위 계산
	Human-in-the loop	- Yahoo's Human review
Resource consumption	돈(Money)	- 메일마다 요금 부과
	시간(Time)	- spammer에게 자동대응(artificial-intelligence-generated) 메일 전송
	메모리	- 워크스테이션에 RAM 추가
	처리(Processing)	- 남용을 방지하기위해 처리 요금 활성화
	대역폭(Bandwidth)	- 데이터 압축 알고리즘
	자원 할당	- 적응형(adaptive)/자동(agile) Agent 시스템
Meta-information	데이터 질 측정	- 조직에 맞는 데이터 품질 관리 가이드라인 제시
	신뢰성있는 메트릭	- Advogato.org
	Currency	- Googlebot/Web crawlers
Data fusion	데이터 축소 및 통합	- Air traffic control, 일기예보
Online community	배타성(Exclusivity)	- Orkut.com
	문화적 표준 및 행동	- Slash.org
Source evaluation	익명 제공 정보	- The Freenet project
	커뮤니티 제공 정보	- 신뢰하고 믿을 수 있는 커뮤니티 시스템
	믿을만한 정보	- 교수 추천 사이트
	하드웨어/소프트웨어 신뢰	- Trusted computing
	인증/테스트	- 소비자가 사람일 때, CAPTCHA(Complete Automated Public Turing Test to tell Computers and Humans Apart) 사용
Structure data	키워드	- 키워드가 포함된 학술적인 논문
	개량된 암호화	- XML
Restricted connectivity	Air-gapped network	- 발전소 네트워크
	P2P 커뮤니티	- Winamp.com
Translating data	효율적인 정보로 변환	- XML 변환
Human computer interface	무결성 보호	- Tripwire
	보전	- Historical archive(Internet WayBack 시스템과 구글 캐쉬)
Locating data	유지방법	- 북마크, 브라우징 히스토리, 간단한 연결
	검색	- 구글
	인덱스	- 야후
	네이밍	- 정보객체에 대한 독특한 이름

의 순서를 이루는 일련의 조작)를 활성화하기위해 마련한 대응수단을 우회하여 스팸이 통과하도록 하는 것이다. 이런 과정이 반복되면서 관련 없는 메일이 메일 수신함에 쌓이게 된다.

이 때 실제 필요한 메일을 확인하기 위해 OODA 루프 모델[14]이 사용된다. 이 모델은 미 공군대령 John Boyd이 제안한 것으로 관찰(Observe), 상황판단(Orient), 결심(Decide), 행동(Act)의 과정을 반복적으로 거치면서 정보를 이해하여 S/N 비율을 분석하는데 도움이 된다는 내용이다.

예를 들어 실제 관심 있는 메일은 5통인데 50통의 메일을 받았다고 가정하자. 즉 45통은 noise이다. 이 45통 중 38통은 명백한 스팸이라고 한다면 나머지는 7통은 좀 더 확인이 필요하다. 이런 확인 과정은 아래와 같다.

- 이메일 헤더를 검색
- 명백한 스팸 제거
- 다음 메일을 읽고, 지울지 보관할지 선택

위와 같은 과정으로 PC(information node)에서 OODA 루프를 50번 수행한다. 매 과정마다 사용자의 시간과 다른 자원들이 소요된다. 특히 확실한 스팸을 지우는 작업보다는 스팸인지를 확신하는 과정의 시간이 더

소요된다. 만일 실제 필요한 메일 확인하고 읽는 시간보다 스팸을 처리하는 시간이 더 소요된다면 DoI 공격이 성공되었다고 할 수 있다. 앞장에서 살펴 보았듯이 DoI 공격의 여러 가지 공격 목적 중의 하나가 인적·물적 가용자원의 소진도 DoI 공격의 목적이기 때문이다.

이런 시간의 소비를 줄이기 위해 여러 가지 대응 수단을 사용한다. 새로운 메일 계정을 만들어 친구들하고만 공유하는 방법(restricting connectivity)도 생각 할 수 있다. 이 때 새로 수신되는 메일을 검사하는 룰을 세우고, 메시지는 예전 메일 계정으로 옮겨가끔 검사를 한다(filtering). 일정 기간 후 새로운 메일 계정이 잘 아는 사람들에게만(exclusivity and restricted connectivity) 알려졌다고 생각될 때 이전 메일 계정은 지워버린다. 그리고 간단한 키보드 작동(interface design)으로 빠르고 효율적인-텍스트 기반 프로그램-스위칭 메일 클라이언트를 고려할 수도 있다.

그리고 스팸을 불법으로 규정하는 몇 가지 법률이 통과했고 요금별납 우편을 통한 스팸이 사업적으로 효율적이지 못하게 하는 것이 고려되고 있다(financial and legal). 그리고 인터넷상의 스팸도 요금을 부과하는 것이 고려되고 있다.

시나리오에서와 같이 스팸 발송자는 정적이지 않다. 그리고 수취인들의 대응 수단을 따라잡기 위해 한 수 위의 대응 수단을 항상 고려한다. 수취인이 이해하기 쉽지만 정보 노드에서 분석하기는 어려운 새로운 방법뿐 아니라 발송인 주소나 이름을 위장하고 악의가 없는 제목으로 메일을 보내 필터링을 우회하려고 항상 노력한다.

Ⅳ. 결 론

본고에서는 현제 네트워크상에서 빈번하게 발생하고 있는 DoI 공격에 대한 여러 가지 동향을 알아보고, 그에 대응하기 위해 제시된 프레임워크에 대해 살펴보았다.

DoI 공격에 대해 정확한 이해를 하고, 효율적인 대응을 하기 위해서는 정보보호에서 다루었던 기밀성(confidentiality), 무결성(integrity), 정보의 가용성(availability) 등의 개념에서 더욱 보강/확장된 보안 요소로서 정보의 규칙성(regularity)과 품질 신뢰(quality trust)같은 metric을 통해 QoI(Quality of Information) 보증(assurance)을 제공해야 한다.

현재 DoI 공격 대응을 위한 산발적인 움직임이 있기는 하지만, 대응하기에는 충분하지 않은 규모이고 명확하지도 않다. 그러므로 본문에서 살펴본 DoI 공격 분류(Taxonomy)와 프레임워크를 기반으로 다양한 공격 시나리오에 대응할 수 있는 분류를 통해 세부적인 대응 연구가 진행되어야 한다.

참 고 문 헌

[1] BcN구축기획단, "정보통신 일등국가 실현을 위한 BcN 구축 기본계획", 정보통신부, 2003.11.

[2] Greg. Conti, "Counting Denial of Information Attacks", Blackhat 2005 & Defcon 13, 2005

[3] "해킹의 프로화 「명예보다 돈이 좋아」", ZDNet Korea, 2004.11.5.

[4] Greg. Conti, Mustaque Ahamad, "A Framework for Countering Denial of Information Attacks", IEEE Security & Privacy, 2005

[5] John Pescatore, "Prevent Targeted Attacks", Gartner, Aug. 2005

[6] Vic Wheatman, "Hype-cycle for Cyber-threats 2005", Gartner Research, Sep. 2005.

[7] "인터넷 신종 사기기법, 파밍(Pharming)", 국가사이버안전센터(NCSC), March 2005

[8] Avivah Litan, "Increased Phishing and Online Attacks Cause Dip in Customer Confidence", Gartner Research, June 2005.

[9] Joris Evers, "DNS servers-an Internet Achilles' heel", CNET News.com, Aug. 2005.

[10] "Phishing Activity Trends Report", APWG, November, 2005.

[11] 최병철, 김국한, 유종호, 서동일, "프로해커 대응방안에 관한 연구", NCS2005,

[12] Mustaque Ahamad, "Guarding the Next Internet Frontier: Countering Denial of Information Attacks", New Security Paradigms Workshop '02, Sep. 2002.

[13] Brian E. Burke, Rose Ryan, "Worldwide Secure Content Management 2005-2009 Forecast Update and 2004 Vendor Shares: Spyware Spam and Malicious

Code Continue to Wreak Havoc", IDC(#34023), Sep. 2005.
[14] G. Hammond, "The Mind of War", Smithsonian Institution Press, 2004.

〈著 者 紹 介〉

김 국 한 (Kook-Han Kim)

2000년 : 한양대학교 물리학과 (이학사)
2003년 : 경희대학교 정보통신대학원 정보통신망관리공학과 (공학석사)
2000 - 2001 : 삼성전자 디지털미디어총괄 컴퓨터시스템사업부 사원
2003 - 2005 : 한국과학기술정보연구원 초고속연구망개발실 연구원
2005 - 현재 : 한국전자통신연구원 네트워크보안구조연구팀 연구원
〈관심분야〉 Network Security, E2E Performance Enhancement, Traffic Measurement

최 병 철 (Byeong-Cheol Choi)

1999년 : 서울시립대학교 제어계측공학과 (공학사)
2001년 : 서울시립대학교 전자전기공학부 (공학석사)
2001 - 현재 : 한국전자통신연구원 네트워크보안구조연구팀 연구원
〈관심분야〉 Network Security, Hacking, Digital Watermarking

유 종 호 (Jong-Ho Ryu)

1998년 : 순천향대학교 전자공학과 (공학사)
2000년 : 순천향대학교 대학원 전기전자공학과 (공학석사)
2004년 : 순천향대학교 대학원 전기전자공학과 (공학박사)
2004~현재 : 한국전자통신연구원 네트워크보안구조연구팀 연구원
〈관심분야〉 Network Security, Cryptography/ Authentication

서 동 일 (Dong-Il Seo)

1994년 2월 : 포항공과대학교 정보통신학과 공학석사
2004년 8월 : 충북대학교 전산학과 이학박사
1989년 1월 ~ 1992년 2월 : 삼성전자 종합연구소
1994년 3월 ~ 현재 : 한국전자통신연구원, 네트워크보안구조연구팀장
2002년 1월 ~ 현재 : ASTAP Forum IS-EG 의장
2003년 1월 ~ 현재 : 정통부지정 IT국제표준화전문가
2004년 1월 ~ 현재 : TTA TC1 부의장
〈관심분야〉 네트워크보안, 해킹, 인터넷정보보호, 보안장비 시험