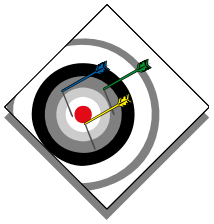


포/커/스

사이버 공격 추적 기술

유종호* 김건량* 김종현** 나중찬***

현재, 해커의 해킹 시도 자체를 제한하는 능동적인 해킹방지 기법과 보안 위배 사고 이후의 법률적 증거 자료 강화 및 책임소재 규명이 사회 전반적으로 요구되고 있으며, 이를 위해 추가 장비 및 신규 네트워크 인프라 변경 없이 라우터 의존성을 배제한 실시간 해커 위치 추적 기술의 중요성이 대두되고 있다. 따라서 기존의 네트워크를 구성하는 라우터에 추가적인 기능 변화 및 IP 헤더에 대한 변경을 수행하지 않으면서도 기존의 ISP(Internet Service Provider)와 연계하여 이기종의 네트워크 환경에서도 사이버 공격 추적이 가능할 수 있는 기술이 필요하다. 본 고에서는 사이버 공격 추적 기술과 관련된 국내외 기술 동향, 표준화 동향, 그리고 국외 대표적인 연구 프로젝트 동향에 대하여 살펴본다. ▨

목 차

* ETRI 보안관제기술연구팀/연구원
** ETRI 보안관제기술연구팀/선임연구원
*** ETRI 보안관제기술연구팀/팀장

Ⅰ. 서 론

새로운 응용 서비스들의 출현과 기존 응용 서비스 품질 수준의 향상에 대한 요구가 급증하면서 네트워크에 대해 점점 정교하고도 고품질을 제공하는 다양한 기능들이 요구되고 있으며, 더불어 개인·기업의 정보와 이용하고 있는 시스템의 보안에 대한 중요성도 예전과 비교할 수 없을 정도로 커지고 있다. 또한 발전하는 응용 서비스와 네트워크 구조에 적합한 보안 기술 즉, 네트워크 차원에서의 적극적인 보안이 가능한 기술의 개발과 도입이 요구되고 있다. 특히 BcN(Broadband Convergence Network) 환경에서는 PSTN(Public Switched Telephone Network), WiBro(Wireless Broadband), WCDMA(Wideband CDMA) 등 다양한 이기종 망이 통합되어 All-IP 기반에서 서비스를 제공하므로 IP 망이 가지는 전통적

인 보안 취약점 및 단일망의 침해사고로 인한 피해가 타 망으로의 급속한 확산 가능성 등이 새로운 문제로 대두되고 있다.

전세계 각국에서는 현재 사이버 공격에 대한 여러 종류의 대응 방안을 모색하고 있으며, 특히 미국은 국가 정보전 차원에서 사이버 공격을 다루고 있다. 현재 우리나라에서도 사이버 공격을 대비하기 위한 정부조직이 창설되어 있으며 각 기업들에 있어서도 사이버 공격의 침입 기술과 대응 기술에 대한 연구가 활발해지고 있다. 그러나 사이버 공격을 자행하는 소위 해커들의 공격 방법도 시간이 지날수록 더욱 정교해지고 고도화되는 것도 사실이다. 이처럼 우리나라에서도 사이버 공격에 대한 대응 방안을 계획하고, 특히, 국가의 사회 간접 자본인 인터넷과 같은 정보통신망을 보호하기 위한 국가 규모의 계획을 수립하는 등 본격적으로 나서고 있지만 아직 미국, 이스라엘 등 기술 선진국에 비하면 크게 뒤쳐져 있다.

현재, 해커의 해킹 시도 자체를 제한하는 능동적인 해킹방지 기술, 보안 위배 사고 이후의 법률적 증거 자료 강화 및 책임소재 규명을 위한 보안기술, 신규 네트워크 인프라 변경 없이(라우터 의존성을 배제한) 실시간 해커 위치 추적 기술 등이 강력히 대두되고 있다. 첨단 정보보호 기술인 능동 보안기술은 기술 선진국의 정보보호에 대한 보호 및 규제로 인해 해외 의존 가능성이 거의 희박하므로 국내의 독자적인 기술 확보가 절실하다 할 수 있다.

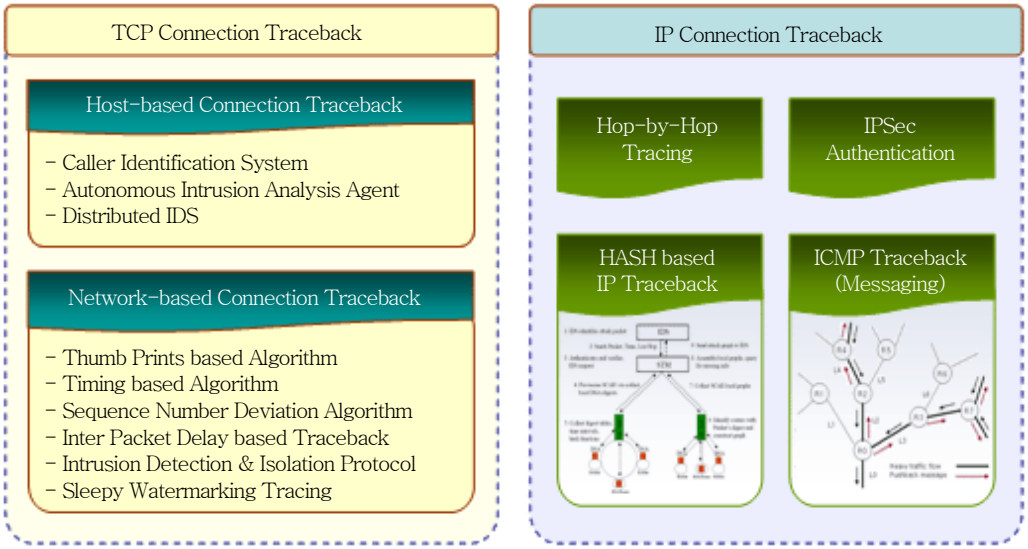
지금까지 살펴본 사항을 토대로, 본 고에서는 향후 사이버 공격이자 위치 추적 기술과 관련한 국내의 기술 동향, 표준화 추진 현황, 그리고 연구 프로젝트 동향에 대해서 살펴보기로 한다.

II. 국내외 기술 동향

사이버 공격 추적 기술은 공격 시스템의 위치와 실제 해킹을 시도하는 해커의 위치가 서로 다르다 하더라도 실제 해커의 위치 즉, 공격의 근원지를 추적할 수 있는 기술을 의미한다. 해킹 시도 자체를 방지하거나 침해사고 발생시 증거확보의 의무화 정책 강화를 위한 사이버 공격 추적 기술은 우회공격을 시도하는 경우의 해커 실제 위치를 추적하는 기술인 TCP 연결 역추적(TCP Connection Traceback or Connection Traceback)과 IP 주소가 변경된 패킷의 실제 송신지를 추적하는 기술인 IP 패킷 역추적(IP Packet Traceback) 혹은 패킷 역추적(Packet Traceback) 등으로 분류된다[1],[2].

현존 추적 기술에는 모든 시스템에 설치한 역추적 모듈을 이용하여 다수의 다른 시스템을 경유한 해커의 실제 위치를 찾아내는 호스트 기반의 연결 역추적 방법, 네트워크 패킷을 감시할 수 있는 위치에 역추적 모듈을 설치하여 다수의 다른 시스템을 경유한 해커의 실제 위치를 찾아

내는 역추적 방법, IP 주소가 변경된 패킷의 실제 송신지를 찾아내는 역추적 방법 등이 제안되어 있으며, 모두 기본적으로 ISP 오버헤드를 감수해야 하는 이론적인 단계이다. 또한 해커 유인용 Honeypot 위장 서버 및 해커 자동 추적 탐지 소프트웨어 등이 개발되어 있으나, 모두 가상 망에서의 특정 환경에서만 운용이 가능한 기술이다[8],[9].



(그림 1) 사이버공격의 역추적 관련 기존 기법

최근 인터넷의 거대화와 더불어 기본적으로 ISP 오버헤드를 최소화하는 요구사항을 만족시켜 줄 수 있는 역추적 기술 보장에 상당히 큰 비중을 두고 있으며, 현재 또는 차세대 인터넷에서 적용 가능한 역추적 기술에 대한 연구가 선진 각국에서 활발히 이루어지고 있다. 특히 선진 각국에서는 많은 위험이 수반될 수 있는 비협력·적대적인 네트워크 환경에서도 동작하고 사이버 공격이 중단된 이후에도 사후처리가 효과적으로 전개될 수 있는 역추적 기술에 역점을 두고 개발에 착수하고 있다.

현재 안전하고 신뢰성 있는 무선 네트워크를 위한 세계의 기술 현황은 디바이스 인증 기술개발에만 주력하고 있으며 무선 네트워크 인프라의 안전성 및 신뢰성 보장을 위한 사이버 공격 감시 및 무선이동 공격 단말에 대한 추적 기술 개발은 태동기이거나 거의 이루어지지 않고 있다.

사이버 공격 추적 기술은 현재 각 자사 제품 위주의 사이트 운영을 통해 제한적이고 수동적인 역추적 기능을 제공하거나 또는 특정 응용 포트에 국한하여 각 응용 서비스 추적 제품을 개발하여 적용하고 있는 단계이다. 주로 웹기반 응용 서비스(웹메일, 웹게시판 등)만을 대상으로

하며, 웹-브라우저의 플러그인을 이용하여 추적을 수행하거나 라우터의 로그를 통계적으로 활용하는 방법이 연구차원에서 수행되고 있다.

전반적으로 감시와 추적 기술은 유·무선 네트워크 인프라 운용과 전술적인 방어 및 통제를 효율적인 수행하기 위한 방법으로 인식되고 있으나, 역추적에 대한 국제적인 공조와 선의의 피해자가 발생할 우려에 대한 사회적·법적 측면에서의 공감대가 형성되어야만 실용적인 기술로 자리매김할 것으로 보인다.

III. 표준화 추진 현황

2007 년, TTA PG102 에서는 현실 망에서 활용 가능한 멀티 도메인간 협업 기반의 공격 추적 수행을 위해 각 도메인 간의 추적 메시지 교환 데이터 형식에 대한 표준화가 표준과제로 채택되어 추진중에 있다.

사이버 공격 추적용 보안이벤트 국제 표준화 동향은 멀티 도메인간 협업을 위해 IETF INCH (INCident Handling) WG 에서 침해사고 데이터 형식인 IODEF(Incident Object Description and Exchange Format), 침해사고 메시지 교환 프로토콜인 RID(Real-time Inter-network Defense)를 표준화가 수행중에 있다. 또한 IETF iTrace WG 에서 ICMP(Internet Control Message Protocol) 메시지를 이용하여 공격 경로 정보를 제공하는 표준화 작업을 진행하여 2000 년에 첫 드래프를 발간하기도 하였으나 2003 년 이후로 작업을 종료하였다. ITU-T 에서는 2007 년 9 월, 차기 회의(2009~2013 년) 기간 동안 추적·감시 관련 국제표준화를 진행하기로 결정하였다.

IV. 연구 프로젝트 추진 현황

실용적인 사이버 공격 추적 기술 실현을 위해 관련한 연구가 전세계적으로 매우 활발히 진행되고 있으며 질적 수준으로 볼 때 연구단계에 놓여진 상태이다. 각 프로젝트들은 공통적으로 ISP 협력 최소화, 기존 프로토콜 의미의 비위반, 추적 분석용 패킷 수의 최소화, 라우터 오버헤드 제거, 핵심 라우팅 구조의 무변경 등과 같은 요구사항을 토대로 진행되고 있다(<표 1> 참조).

국내의 보안업체들은 공격자 추적 기술을 이용한 IDS, Firewall, IPS 등의 제품의 형태로 TRIOPS 사의 Stealth Tracking(웹서버)/Mail, 해커스랩의 N-Patrol 과 아이자이어 로보텍스사의 TraceView 가 대표적인 관련 제품을 개발하여 출시하였으며, 주로 L7 추적 메커니즘에 무게중심을 둔 제품들이 출시되어 있다[6](<표 2> 참조).

<표 1> 국외 사이버공격 추적 기술개발 동향

기관 또는 프로젝트	연구내용
DETER (cyber DEfense Technology Experimental Research)[3]	- 미국의 국가과학기금(National Science Foundation: NSF)과 국토안보국(Department of Homeland Security: DHS)에서 지원을 받고 있으며, UC Berkeley 와 USC-ISI 주관으로 미국 내 우수대학·보안업체·정부연구기관과 함께 네트워크 인프라 마비공격에 대한 감시 및 추적 기술을 연구중에 있음 - USC/ISI, UC Berkeley, McAfee(NAI) 연구소 등이 주관으로 사이버 공격 대응 및 방어에 대한 연구를 수행함에 있어 현실적인 시나리오에서 새로운 이론과 기술을 테스트할 수 있는 테스트베드 구축에 대한 연구를 수행중이며, 미국의 Utah 대학에서 개발한 'Emulab'이라는 클러스터 테스트베드 기술을 적용하고 있음
EMIST (Evaluation Methods for Internet Security Technology)[4]	- EMIST 는 DETER 프로젝트의 테스트베드 구축을 위한 부분 연구과제로서 실험적 보안데이터의 정의, 제어 및 분석을 수행하는 테스트베드용 GUI 를 개발하고 있으며, Penn State, McAfee Research, ICSI, Purdue, SPARTA Inc., SRI International, UC Davis 등과 같은 산·학·연의 공동연구기관에 소속된 DETER 프로젝트의 초기 멤버들로 구성됨 - DDoS, 웜 전파, BGP 라우팅 공격등과 같은 네트워크 공격의 분류와 감시 및 추적에 대한 테스팅 프레임워크 및 방법론을 연구하고 있음
Network Attacks Traceback[5]	- 미국방부 공군연구소 주관으로 ARDA(Advanced Research and Development Activity)와 함께 2006 년부터 네트워크 공격 역추적 기술개발을 목적으로 만들어졌으며, 3 년간 100 억 원의 펀드를 조성하여 미국 내 우수대학들과 공동으로 시제품 개발을 진행중임 - 정보기관(Intelligence Community: IC) 네트워크에 정보의 기밀성 그리고 완전성을 손상시키는 공격에 대한 역추적 기능을 수행하기 위해 비협력 그리고 적대적인 네트워크 환경을 고려한 고위험도 또는 고지불 기능이 포함된 기술을 개발하는 것이 목표임 - IC 네트워크에서 발생할 수 있는 서비스 거부 공격(DoS)에 대한 역추적 기술과 확률적 패킷 마킹 기법을 이용한 역추적 기술은 배제하며, 기존 프로토콜의 규칙에 위반되지 않고 핵심 라우팅 구조의 변경 없이 동작이 가능해야 하며, 공격자가 추적 현황을 탐지하기 어렵고 공격이 끝난 이후에도 사후처리로 효과적으로 전개가 가능한 기술개발을 진행중임
Tracing Attacks through Non-Cooperating Networks	- SPARTA 연구소의 주관으로 기술적 제약이 많은 인터넷 환경에서 공격감시 및 추적 기술에 대한 여러 가지 방법들을 개발하고, 분산된 모니터링 노드 간의 협력을 지원하기 위하여 CITRA 기반의 추적기술을 연구중임 - 1 차 목표로 개발중인 DETER 프로젝트 환경에서 다양한 소프트웨어 기반의 전송장비(예; NAT devices, proxies, interactive login stepping stones, encrypting/decrypting gateways)를 구성하여 테스트베드를 구축하고, 실시간 공격추적 기술을 시험 계획
NVAC (National Visualization and Analytics Center)[7]	- 미 국토안보부 주관의 NVAC 은 각 대학 등 공동으로 사이버 네트워크의 테러 징후를 발견하는 것을 목적으로 하며 보안이벤트을 시각적으로 표시하기 위한 방법을 중점적으로 연구중임
일본 NiCT Information Security Research Center[10]	- NiCT(National Institute of Information and Communication Technology)에서 spoofing 과 reflection 공격들에 대한 해결책뿐만 아니라 추적 메카니즘을 개발

<표 2>의 모든 제품은 웹기반 응용 서비스(웹메일, 웹게시판 등) 만을 기본으로 수행하는 점에 있어, 향후에는 웹을 포함한 주요 응용 서비스와 이용자를 대상으로 확장될 것으로 기대된다.

<표 2> 사이버공격 감시 기술개발 동향

제품	내용
TRIOPS 사의 STEALTH TRACKING(웹서버)	알려진 포트(80 번)를 통한 침입을 탐지하고, 침입자의 위치 정보를 실시간으로 파악할 수 있는 웹 기반의 침입자 위치 추적 시스템과 STEALTH MAIL 이라는 전자우편의 수신자가 메일을 확인하는 즉시, 수신자의 위치 파악이 가능
해커스랩의 N-Patrol	불법 침입의 실시간 탐지와 자동 차단 그리고 경보에 이은 즉각 대응기능 등 보안 관제 서비스 기능과 실시간으로 침입자의 시스템을 바로 추적하여 그 위치를 관제센터에 전송
아이자이어 로보텍스사의 TraceView	각종 웹서비스에 대한 접근 및 로그인 행위자에 대해 각종 IP 위장시라도 사설 IP 까지 실시간 자동 추적을 가능하게 하고, 차단 정책과 일치 시 해당 세션을 차단하고 실시간 모니터링하는 기능을 제공
HightTower Software's TowerView	NASA 의 우주항공 구성요소들의 추적 기술 등을 기술이전 받아 상용화하였으며, 방대한 데이터가 존재하는 망관리 등에 시각적인 상황인지 기술을 적용하였음
ETRI's VisualScope	2005 년부터 직관적인 네트워크 보안상황을 인지하기 위해 논리적・물리적 위치기반의 보안이벤트 시각화 기술을 연구함
CMU	1998 년 11 월 DARPA(Defense Advanced Research Projects Agency)에 의해 구성된 CERT(Computer Emergency response team)에서 NetSA(Network Situational Awareness) 그룹을 만들어서 전반적인 네트워크 활동을 분석하고 모니터링 및 시각화를 위한 기술적 해결책과 연구방법을 개발하고 있음. 특히 FloCon 이라는 Workshop 을 통해 연구결과들을 공유

Ⅴ. 결 론

지속적인 해킹과 비정상행위의 원인규명을 위한 공격에 대한 추적 기술 연구는 전자금융거래법 시행과 함께 시기상으로 요구되고 있다. 또한 안전하고 신뢰성 있는 무선 네트워크를 위해 디바이스 인증 기술개발에만 주력하고 있으며, 무선 네트워크 인프라의 안정성 및 신뢰성 보장을 위한 공격 감시 및 추적 기술 개발은 이루어지지 않고 있다. 무선 네트워크에서의 이동단말을 이용한 공격자는 이동성 및 은닉성을 극대화하여 액세스망 영역에서 퓨전 웜 등을 유발할 수 있으므로 새로운 실시간 감시 기술을 이용하여 신속하고 효율적인 사이버 공격 대응 기술이 필요하다.

현재 추적 기술은 현실 망에서 활용하기 위한 연구개발 초기 단계이며, 향후 사이버 공격에 대한 실시간 추적 연구는 유무선 환경에서 적응 가능한 멀티 도메인간 협력 기반 또는 비협력 기반 공격자 병렬 추적 기술로 진화될 것으로 전망되며, 네트워크 기반 구조나 운영상의 변화 관점의 ISP 부담 최소화 및 모든 네트워크 프로토콜 기반의 역추적 기술이 개발될 것으로 추정된다.

특히, 실시간 추적 기술은 다양한 인프라 환경과 융합 공격을 포함한 돌발 상황에 적응 가능하도록 멀티 도메인 간에 협업화하여 공격자를 병렬로 추적, 이는 무선 네트워크 환경의 무선 단말기기까지 확장 가능할 것으로 기대된다. 현재의 공격자 추적 기법은 아직까지 실제 인터넷

에 적용하여 사용하기에는 도메인간 정보공유에 따른 많은 기술적 제약조건들이 있다. 따라서 인프라의 마비, 해킹을 통한 내부 정보의 유출, 은닉성(undetected) 공격 등과 같은 치명적인 공격들에 대한 효과적인 대응을 위해, 이종의 보안장치간, 이종의 네트워크간, 이종의 사업자간의 안전한 상호 연동형 서비스 환경을 제공하는 것이 무엇보다 중요하며, 다양한 수준의 감시 및 추적 시나리오를 침입 탐지 기술, 대응 복구기술과 연계하여 사이버테러에 대해 자동화된 대응 체제 구축이 가능할 것으로 기대된다.

전세계에서 유무선 통합의 움직임을 보이는 등 유무선 통합의 All-IP 환경은 거스를 수 없는 대세이며, 이에 따라 무선 단말기기를 포함하여 은닉성 공격에 대한 감시 및 추적 기술의 필요성은 더욱 증대될 것으로 예상된다.

<참 고 문 헌>

[1] 이재광, “역추적 기술 동향,” 전자정보센터, 2005. 1.
[2] 한국기술거래소, “네트워크 침입자 역추적기술 동향,” 전자정보센터, 2004. 10.
[3] DETER 프로젝트, http://www.isi.edu/deter/
[4] EMSIST 프로젝트, http://www.csl.sri.com/projects/emist/
[5] Network Attacks Traceback 프로젝트, http://www.ic-arda.org/
[6] SecureScope, Secure Decisions, http://www.SecureDecisions.com/
[7] 미국국토안보국 NVAC, http://nvac.pnl.gov/
[8] Alex C. Snoeren, Craig Partridge, Luis A. Sanchez, Christine E. Jones, Fabrice Tchakountio, Stephen T. Kent, and W. Timothy Strayer, “Hash-based IP Traceback,” ACM SIGCOMM'01, 2001. 8.
[9] Stefan Savage, David Wetherall, Anna Karlin, and Tom Anderson, “Practical network support for IP traceback,” ACM SIGCOMM’00, 2000. 8.
[10] NiCT 정보보호연구센터, http://www.nict.go.jp/

* 본 내용은 필자의 주관적인 의견이며 IITA 의 공식적인 입장이 아님을 밝힙니다.