http://www.jsebs.org
ISSN: 2288-3908

The Journal of Society for e-Business Studies
Vol.22, No.4, November 2017, pp.129-139
https://doi.org/10.7838/jsebs.2017.22.4.129

IP 마킹 서버를 활용한 금융 전산망 공격자 역추적 기술 연구

A Study on Trace-Back Method of Financial Network Using IP Marking Server

박근호(Keunho Park)*, 최규원(Ken Choi)**, 손태식(TaeShik Shon)***

초 록

핀테크의 등장으로 인하여 많은 금융 서비스가 모바일 인터넷 환경에서 이용할 수 있게 되었고, 최근에는 온라인으로 모든 은행 서비스를 제공하는 인터넷 은행도 생겼다. 이처럼 인터넷을 통한 금융 서비스의 비중이 늘어남에 따라 사용자들에게 편의를 제공하지만 그와 동시에 금융 전산망에 대한 위협도 증가하고 있다. 이에 따라, 금융 기관들은 침해사고에 대비하여 보안시스템에 많은 투자를 하고 있지만 날이 갈수록 해커에 의한 공격은 정교해지고 있어서 대응하기 어려운 경우도 많다. 본 논문에서는 공격자의 실제 위치를 파악할 수 있는 IP 역추적 기술을 살펴보고 금융 전산망 분석을 통해 IP 역추적 기술을 적용하기 위한 다양한 방안을 제시한다. 그리고 Infra-Structure 구축을 통한 새로운 IP 역추적 방법을 금융 전산망에 적용하는 방법을 제안하고 시뮬레이션을 활용한 실험을 통해 효율성을 증명하고자한다.

ABSTRACT

With the advent of FinTech, many financial services have become available in the mobile Internet environment and recently, there is an internet bank that provides all bank services online. As the proportion of financial services over the Internet increases, it offers convenience to users, but at the same time, the threat of financial network is increasing. Financial institutions are investing heavily in security systems in case of an intrusion. However attacks by hackers are getting more sophisticated and difficult to cope with. However, applying an IP Trace-back method that can detect the actual location of an attacker to a financial network can prepare for an attacker's arrest and additional attacks. In this paper, we investigate IP Trace-back technology that can detect the actual location of attacker and analyze it to apply it to financial network. And we propose a new IP Trace-back method through Infra-structure construction through simulation experiments.

키워드 : 금융 전산망, 공격자 역추적, IP 패킷 마킹
Financial Network, Trace-back, IP Packet Marking

본 연구는 미래창조과학부 및 정보통신기술진흥센터의 대학ICT연구센터육성 지원사업의 연구결과로 수행되었음(IITP-2017-2016-0-00304).

* First Author, Department of Computer Engineering, Ajou University(happyrjsgh19@gmail.com)
** Second Author, Department of Electrical and Computer Engineering, Illinois Institute of Technology (kchoi@ece.iit.edu)
*** Corresponding Author, Department of Cyber Security, Ajou University(tsshon@ajou.ac.kr)
Received: 2017-11-02, Review completed: 2017-11-19, Accepted: 2017-11-14

1. 서 론

최근 금융 기관을 대상으로 개인정보 탈취, 분산 서비스 거부 공격과 같은 침해사고가 많이 발생하고 있다. 금융 기관에 있어서 침해사고로 인한 서비스 장애는 고객의 신뢰도 하락과 함께 금전적인 피해로 직결될 뿐만 아니라 해당 공격 루트를 이용한 추가적인 공격이 발생할 가능성이 있기 때문에 치명적이다. 그렇기 때문에 침해사고의 근본적 원인인 공격자를 색출하지 않는 이상 지속적인 피해가 발생할 것이다[5, 7].

따라서 금융 기관에서는 해커의 위치를 추적하여 빠른 시간 내로 피해가 커지는 것을 방지하고 나아가 해커로 하여금 공격 의지를 상실하게 하는 능동적인 보안 기술이 요구되고 있다.

본 논문에서는 금융 기관의 전산망 구조를 분석하고 능동적인 보안 시스템을 적용하기 위한 역추적 기법에 관해 연구했다. 제 2장에서는 기존에 제안된 IP 역추적 방법들을 특징에 따라 분류하여 설명한다. 제 3장에서는 금융 전산망에 적용하기 위한 역추적 시스템에 관하여 제안하고 제 4장에서는 제안하는 역추적 방법과 기존의 역추적 기법들을 실험한다. 마지막으로 제 5장에서는 결론 및 향후 수행되어야 할 과제에 관하여 논의한다.

2. 관련 연구

이번 장에서는 금융 전산망에 효율적으로 적용할 수 있는 IP 역추적 방법을 개발하기 위해, 기존 패킷 마킹 연구들에 대한 분석 내용을 논의한다. 이 분석 내용을 활용해 기존 기법들의 한계점을 보완한 방식으로 논문에서 제안하는 기법에 활용된다.

2.1 PPM

PPM(Probabilistic Packet Marking)은 라우터를 지나는 패킷에 라우터를 식별하는데 필요한 몇 가지 정보를 특정한 확률로 마킹하는 기술로 2000년도에 D. Wetherall, Savage에 의해 처음 소개되었다[9]. 이 방법은 서비스 거부 공격과 같은 발신지의 주소를 속이고 공격 트래픽을 보내는 공격의 최초 공격 발생지를 찾는데 효율적이다. 공격 트래픽의 발신지를 알아내기 위해서 엣지 라우터에서는 일정한 확률로 라우터의 주소를 IP 헤더의 identification 부분에 표시한다. 그 후, 피해가 발생하였을 때 패킷의 IP 헤더를 분석하여 공격이 최초로 발생한 지점까지의 경로를 재구성하여 식별할 수 있다. 패킷에 마킹할 확률 p, 소스에서 목적지까지 홉의 수 d, 주소의 fragment 수를 k라고 하면 공격자의 경로를 예측하기위해 필요한 총 패킷의 수는 아래의 식 (1)을 통해 예측할 수 있다.

$$E(X) < \frac{k \cdot \ln(kd)}{p(1-p)^{d-1}} \quad (1)$$

PPM은 엣지 라우터의 ID fragment를 재구성하기 위한 순열과 조합이 너무 많다는 단점이 있다. 또한 라우터가 공격자에 의해 변조되어있을 경우 무용지물이 된다는 단점도 존재한다.

2.2 DPM

DPM(Deterministic Packet Marking)은 2003년 Andrey Belenky에 의해 소개되었다[2]. DPM은 패킷의 소스와 가장 근처에 있어 패킷 마킹에 사용되는 엣지 라우터를 최소 단위로 취급하던 PPM과는 달리, 엣지 라우터 하나의 인터페이스를 최소 단위로 규정하였다. 인터페이스를 추적의 최소 단위로 함으로써 라우터를 향해 들어가는 패킷과 나가는 패킷을 구분할 수 있어 라우터를 향해 들어오는 패킷만 마킹한다. 또한 PPM과 구분되는 가장 큰 차이점은 네트워크에 진입하는 모든 패킷을 마킹한다는 점이다. 하지만 마킹해야 할 인터페이스의 IP 주소는 32비트이고 마킹에 활용될 IP 헤더의 Identification 부분과 Flag의 크기는 총 17비트이므로 마킹할 공간이 부족하다. 그래서 라우터 인터페이스의 IP 주소를 임의의 수로 나누어 랜덤으로 기록한다. DPM은 모든 패킷을 마킹함으로써 공격자가 mark spoofing을 하더라도 원래의 라우터 정보를 덮어 쓰기 때문에 PPM과 비교했을 때 더 안전하다고 할 수 있다.

2.4 DFM

DFM(Deterministic Flow Marking)은 2013년 캐나다 Dalhousie 대학의 Vahid Agheai Foroushani에 의해 제안된 기술이고 PPM, DPM과는 다른 방식으로 마킹을 한다[4]. source IP 주소, destination IP 주소, Layer 4 프로토콜 타입(TCP/UDP, ICMP), source 포트, destination 포트를 하나의 Flow ID라 하고, 두 개의 네트워크에서 통신할 때 패킷 지연시간 내에 전송되는 Flow ID가 같은 단방향 시퀀스를 Flow라고 하여 Flow마다 마킹하는 기법을 제시하였다. 또한 라우터가 탈취당해 공격자가 임의의 마킹 값을 넣어 패킷을 변조하는 경우를 대비하여 ECDSA를 사용한다. 각 엣지 라우터는 ECDSA 공개키를 공유하고 각각의 Flow마다 서명을 생성한다. 그 후 42바이트의 ECSDA 전자 서명을 임의의 패킷 페이로드 제일 마지막에 추가하고 피해자 측에서는 패킷 검증 여부를 저장하는 테이블을 만들어 관리한다.

3. 금융망을 위한 역추적 방안

이번 장에서는 전자금융 전산망이 공격자에 의해 공격을 받을 경우 공격자의 위치를 알 수 있는 방법에 관해 연구했다. 이를 위해 기존의 역추적 방법들을 비교 분석하여 금융 전산망에 적용할 수 있는 가능성에 관해 알아보고 금융망에 적합한 공격자 역추적을 위한 신규 인프라를 추가하는 방안을 제안한다.

3.1 기존 기법을 활용한 방안

금융 전산망이 공격자의 정보를 식별하기 위해서는 기존의 역추적 기법인 패킷 마킹 기법을 활용할 수 있다. 이때 패킷의 근원지를 식별할 수 있는 정보를 삽입하기 위해서 IP헤더 구조에서 Identification field를 활용할 수 있다[8]. Identification field는 하나의 패킷이 여러 조각으로 분할되었을 경우 각 조각을 구분하기 위하여 부여되는 정보이다. 하지만 네트워크 계층에서 수신자가 단편화된 IP패킷을 받고, 이 패킷들에 대한 재전송을 요구할 경우 상당

히 많은 양의 패킷을 재전송해야 하므로 네트워크 계층의 단편화는 end-to-end 성능에 좋지 않은 영향을 미칠 수 있다. 이러한 이유로 약 0.25% 정도의 패킷만 단편화 된다는 연구결과가 있으며 결과적으로 Identification field를 마킹을 위해 사용하여도 기존의 프로토콜과 원활하게 상호 운용될 수 있다[10]. PPM과 DPM, DFM을 활용하여 아래와 같은 정보를 패킷에 마킹할 수 있다.

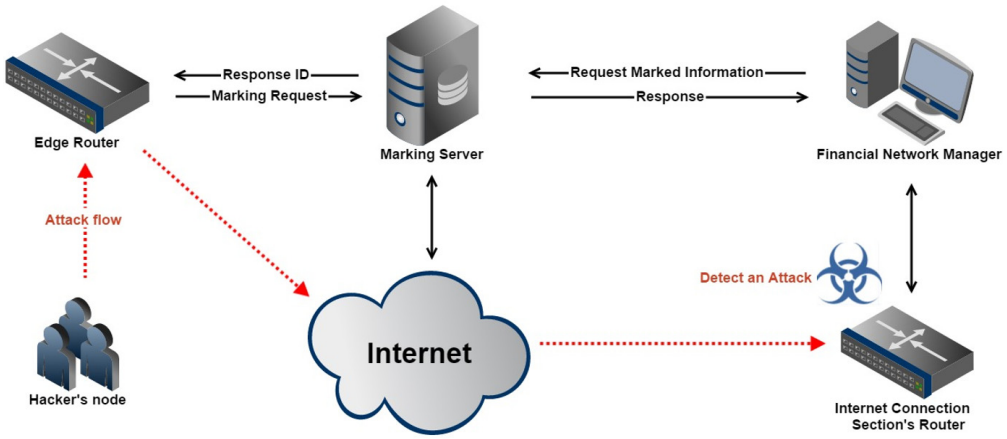
(1) 엣지 라우터의 정보(32bit): 엣지 라우터는 공격에 사용되는 노드와 가장 가까이 있으며 egress 인터페이스의 주소가 할당된 라우터를 의미한다. 라우터가 로컬 네트워크에서 패킷을 받고 목적지의 IP 주소를 읽어서 라우팅 경로를 결정한 뒤 egress 인터페이스를 통해 다음 라우터로 향하게 되는데 이때 egress 인터페이스의 정보를 마킹함으로써 공격에 사용된 노드가 사용한 라우터의 위치를 알 수 있다.

(2) MAC 주소 고유 번호(48bit): 라우터가 MAC 필터링을 수행하여 라우터에 등록되지 않은 노드의 MAC 주소는 허용하지 않는다고 가정할 경우 패킷이 라우터의 egress 인터페이스를 통해 네트워크로 흘러가기 이전에 노드의 고유번호를 알 수 있는 MAC 주소가 egress 인터페이스의 주소로 바뀐다. 그러므로 라우터에서 패킷에 MAC 주소를 식별할 수 있는 정보를 마킹하여야 한다.

(3) Fragment Indicator: 엣지 라우터 정보 또는 공격자 노드의 MAC 주소를 단일 패킷에 마킹하여 전송하기엔 패킷에 마킹할 수 있는 공간이 제한되어있다. 그러므로 일정 단위로 잘라서 마킹해야 하는데 이때 Fragment Indicator를 통해 순서를 구분할 수 있다.

기존 기법들의 금융망 적용 가능성을 비교하기 위한 항목들로는 호환성, 실시간성, 오버헤드 최소화, 필요 패킷 수, 유연성이 있으며 각 항목에 대한 설명은 아래와 같다.

- **호환성**: 기존의 네트워크 환경 및 프로토콜과 호환이 되어야 한다.



〈Figure 1〉 The Structure of the Proposed Trace-Back System

- **실시간성**: 실시간으로 공격자 역추적이 가능해야 한다.
- **오버헤드 최소화**: 역추적을 위한 오버헤드로 인해 네트워크 트래픽이 증가하는 정도이다.
- **필요 패킷 수**: 공격자의 실제 위치를 추적하는데 필요한 패킷의 수, 적을수록 좋다.
- **메모리 요구**: 역추적 정보를 저장하는데 필요한 메모리의 크기가 작아야 한다.
- **유연성**: 공격자의 수가 증가하여도 정확성을 유지하여야 한다.

금융 전산망의 특성상 ATM, 공과금 수납기, 순번 대기표 등 다양한 End Point가 존재한다. 기존의 패킷 마킹 기법을 금융 전산망에 적용할 경우, 금융 서비스 사용자부터 금융 전산망의 서버로 가는 경로에 있는 라우터 뿐 아니라 다양한 End Point 또한 고려하여 패킷 마킹 기능을 지원해야 하므로 호환성 측면에서 성능이 떨어진다. 또한 금융 전산망은 금융 서비스를 제공하는 웹 서버가 위치한 DMZ 구간과 외부 트래픽을 받는 인터넷 연결구간이 IDS와 방화벽으로 망 분리되어 운용되고 있어 웹 서버를 대상으로 하는 직접적인 공격에 비해 인터넷 연결 구간을 대상으로 하는 DDoS 공격에 취약하다. 이러한 금융 전산망의 특성을 고려했을 때, DDoS 공격이 발생할 경우 기존의 IP 역추적 기법은 이미 전송된 패킷을 분석하여 경로를 재구성해서 근원지를 찾으므로 실시간으로 C&C 서버를 추적하여 차단하기 힘들다. 오버헤드와 필요한 패킷 수의 경우 PPM과 DPM에 비해 패킷의 Flow 단위로 마킹을 하는 DFM이 적은 수의 패킷으로 공격자의 위치를 재구성할 수 있으므로 더 효율적이다. 결과적으로 필요한 DFM 패킷의 수가 적기 때문에 라우터에서 식별을 위해 저장하기 위해 요구되는 메모리의 크기도 적고 그만큼 여러 명의 공격자가 존재하여도 수용할 수 있는 유연성이 좋다고 할 수 있다.

3.2 새로운 Infra-structure를 추가 하는 방법

이번 장에서는 기존의 역추적 기법들을 금융 전산망에 적용했을 때 발생하는 단점을 보완하기 위해 Infra-structure를 추가하는 방법을 제안하고 실제 금융 전산망에 적용할 수 있는 방안에 관해 논의한다.

제안하는 방법은 Infra-structure로써 마킹 정보를 관리하는 마킹 서버를 ISP에 구축한다. 이러한 마킹 서버는 ISP 곳곳에 위치하고 있고, 하나의 메인 마킹 서버가 존재하여 각각의 ISP에 존재하는 마킹 서버들의 역추적 정보를 취합하여 공유, 관리한다. 엣지 라우터는 기밀성과 무결성을 보장하기 위해 공개키 암호화 알고리즘을 사용하여 마킹 서버와의 통신을 통해 역추적에 필요한 정보를 전송한다. 이때 전송되는 정보는 엣지 라우터의 주소와 노드의 IP, MAC 주소, 패킷을 식별할 수 있는 고유번호이다. 라우터는 15bit의 고유번호를 패킷에 마킹하여 라우팅하고 동시에 마킹서버로 전송한다. 또한 기존 금융 전산망의 인터넷 연결 구간에는 공격을 받을 경우 마킹 서버에게 공격자의 정보를 요청하는 쿼리를 보내는 클라이언트를 구축한다. 제안하는 역추적 시스템의 구조는 <Figure 1>과 같으며 절차는 아래에 설명하였다.

(1) 엣지 라우터에서 패킷을 전송할 때, 최종 목적지가 등록된 금융 기관의 IP일 경우, 네트워크 계층에서 확인할 수 있는 DDoS 공격 유형 체크 등 유해 패킷 검사를 수행한다. 만약 의심스러운 Flow가 탐지되면 Flow의 정보와 함께 마킹 서버에 마킹 요청을 보낸다.
(2) 엣지 라우터로부터 마킹 요청을 받은 마킹 서버는 패킷 Flow의 정보를 데이터베이스에 저장하고 해당 Flow의 고유 식별번호를 생성하여 엣지 라우터로 관련 정보를 전송한다.
(3) 엣지 라우터는 의심스러운 Flow의 마킹 가능한 필드에 마킹을 시작한다.
(4) 만약 금융 전산망의 인터넷 연결구간에서 공격을 받거나 탐지했을 경우, 패킷의 Flow 고유 식별번호가 마킹된 부분을 확인하여 마킹 서버에게 피해 확인 요청을 보낸다.
(5) 마킹 서버는 고유 식별번호와 Flow의 정보를 확인하여 공격자와 가장 가까이 있는 라우터의 주소와 공격자 노드 정보를 금융 전산망 관리자에게 알려준다. 그러면 금융 전산망에서는 공격자 정보를 활용하여 조치를 취할 수 있다.

위와 같은 방법으로 금융 전산망 공격자 역추적을 위한 Infra-structure를 구축할 경우 기존의 역추적 방법에 비해 역추적에 필요한 정보를 오랜 시간 많은 데이터를 보관할 수 있기 때문에 금융 전산망 침해사고가 발생할 경우, 네트워크 포렌식 측면에서 효율적이다. 또한, 금융 전산망이 DDoS 공격을 받을 경우 네트워크 자원을 많이 소모하기 때문에 기존의 역추적 방법의 경우 역추적과 관련된 모든 트래픽 분석과 네트워크 경로의 재구성이 힘들다. 반면, 제안하는 방법의 경우 피해자의 네트워크 자원의 부담을 덜어주기 때문에 공격자 역추적에 대한 확장성을 보장해 준다.

또한, 역추적을 담당하는 서버에서 금융 전산망을 대상으로 하는 공격 패킷의 정보를 관리한다. 그러므로 공격 경로를 재구성함으로써 ISP 네트워크 위상 및 금융 전산망의 구조를 공개하지 않아도 된다. 이러한 이유로 금융 IT 보안의 이슈인 제3자 또는 내부자에 대해 보안성이 증대되며 공격 재발 방지에 효율적이다.

3.3 금융 전산망에 Infra-structure 적용 방안

본 절에서는 본 논문에서 제안하는 공격자 역추적을 위한 새로운 Infra-structure를 구축하는 방법을 실제 금융 전산망에 적용하여 활용하는 방안에 관해 논의한다.

3.3.1 금융공동망에 적용하는 방안

금융공동망이란 금융결제원이 구축하고 운영하는 지급결제시스템으로 다양한 금융기관과 금융결제원의 전산시스템을 상호 연결하여 금융 이용고객에게 각종 금융거래 서비스와 금융거래 정보를 제공한다. 금융공동망은 현금자동인출기 공동망, 타행환 공동망, 전자금융 공동망, 은행간 공동 정보망 등으로 구성되어 금융 서비스 이용고객이 거래은행에 가지 않고도 각종 서비스를 사용할 수 있다.

금융공동망은 일반 인터넷 네트워크와 달리 물리적으로 분리되어 운용된다. 금융공동망에서 통신에 사용되는 프로토콜의 경우, 기존에

사용되던 X.25는 네트워크 효율성의 이유로 현재 TCP/IP로 전환되었다. 또한 금융공동망을 사용하는 각 주체들 간의 통신의 경우, 기존에 정의된 서비스를 위한 통신에 한정되어 있고, 디바이스의 경우도 사전에 등록된 기기를 사용하여 인터넷 네트워크에 대비해 규칙성을 보인다.

이러한 금융공동망의 특징을 고려하여 제 4.2절에서 제안한 방법을 적용할 경우, 역추적을 위한 라우터와 마킹 서버의 구축비용이 일반 인터넷 네트워크에 비해 규모 측면에서 저렴하고 수용 가능한 범위 내에 있기 때문에 실현 가능성이 높다. 또한 네트워크 계층에서 TCP/IP 프로토콜을 사용하므로 IP Header의 Identification field을 활용하여 거래고유 번호 마킹을 통해 spoofing을 방지할 수 있다. 정해진 서비스와 규칙적인 통신을 한다는 특성을 활용하여 Flow 단위 마킹이 아닌 서비스 단위 마킹이 가능해지며 이로 인해 IP 패킷 마킹과 관련된 오버헤드를 줄일 수 있다.

또한 전자금융 사기 방지를 위해 활용할 수 있다. 최근 대포통장 단속이 강화됨에 따라, 가상계좌를 피싱(Phishing) 수단으로 활용하는 사례가 증가하고 있는 추세이다. 가상계좌란 실존하는 계좌에 연결된 계좌로 실제 통장이 존재하지 않고 단지 계좌번호만 고객의 이름으로 부여받는 계좌이다. 가상계좌는 금융실명제와 상관없이 거래할 수 있으며, 가명으로 사용되며 수시로 번호를 바꿀 수 있어 모(母)계좌 소유주를 찾지 못하면 송금자를 알 수 없어 범죄에 악용될 수 있다.

이러한 문제는 역추적을 위한 Infra-structure가 적용된 금융 전산망을 통해 해결할 수 있다. 가상계좌와 거래하는 ATM 등 여러 종류의 End Point에서 피해자가 송금하거나 공격자가 출금하는 통신과정에서 발생하는 패킷에 가상계좌 고유 사용자를 식별할 수 있는 ID를 마킹하고 관련 정보를 마킹 서버에 전송한다. Phishing 공격에 가담된 공격자와 관련된 End Point 정보는 마킹 서버를 통해 조회할 수 있기 때문에 공격자가 다양한 경로를 통해 추적을 피하려고 시도하더라도 추적할 수 있다. 뿐만 아니라 금융전산망 역추적 시스템을 홍보할 경우 전자금융 사기 시도 자체가 줄어들 것으로 예상된다.

3.3.2 다양한 금융 거래 프로토콜과의 연동

주식, 선물, 옵션, 채권 등 다양한 금융 상품들을 거래하기 위한 표준 프로토콜인 FIX(Financial Information Exchange), 장외파생시장에서 상품거래에 사용되는 표준 프로토콜인 FpML(Financial products Markup language), 글로벌 금융거래 정보를 안전한 환경에서 교환할 수 있게 은행과 기타 금융기관 간 연결네트워크를 제공하는 SWIFT(Society for Worldwide Interbank Financial Telecommunication) 등 다양한 금융거래와 관련된 프로토콜이 개발되어 전 세계적으로 금융관련 기관에서 사용된다. 금융기관들은 금융 거래 프로토콜을 사용함으로써 전자 금융 거래의 편의성, 확장성 등을 제공받는다. 또한 이러한 프로토콜은 각 프로토콜을 사용하는 금융기관의 목적에 따라 다양한 금융정보들이 Application 계층에서 표준에서 정의한 형식을 바탕으로 통신 한다는 공통점이 있다. 하지만 금융거래 표준 프로토콜을 사용한 통신은 금융거래와 직결되기 때문에 다양한 공격자로부터 공격의 대상이 되기도 한다. 사례를 통해, 위에서 소개한 금융

거래 프로토콜 중 하나인 SWIFT 전산망에서 발생한 침해사고 경위를 설명하고 금융 거래 프로토콜의 특성과 본 논문에서 제안하는 IP 마킹 서버에 금융 거래 프로토콜을 고려하여 맞춤형 기능을 적용하는 방안에 관해 설명하겠다.

2016년 2월 방글라데시 중앙은행이 뉴욕 연방준비은행에 예치해 둔 한화 1167억 원 상당이 해킹으로 인해 사라진 사건이 발생했다. 미국의 보안업체인 FireEye 社의 보고서에 따르면, 알 수 없는 경로를 통해 방글라데시의 SWIFT 전산 시스템을 해킹하기 위한 악성 코드를 침투시켜 은행서버 컴퓨터가 감염된 것으로 보고 있다. 공격자는 감염된 컴퓨터를 통해 알아낸 SWIFT 시스템의 로그인 정보를 활용하여, SWIFT 망으로 이체 메시지를 보내어 필리핀 은행을 통해 돈을 인출하였다. 또한, 사용된 악성코드에서 KB국민은행을 포함한 8개 은행의 SWIFT 코드가 발견되었는데, 이는 악성코드에 감염된 SWIFT 단말에서 국민은행 등 8개 은행의 SWIFT 코드로 자금을 이체할 경우 중간 가로챌 목적을 염두에 둔 것으로 예상된다.

이와 같은 금융 전산망 침해사고 사례를 통해, 금융거래 프로토콜의 특성을 고려한 IP 역추적 서버 구축의 필요성을 알 수 있다. 따라서 본 논문에서 제안하는 방식에 각 금융 거래 프로토콜에서 사용되는 메시지 Type, Price, End Point 정보, 금융거래정보 필드, 개인 식별 ID 등을 이상행위 식별에 도움이 되는 정보를 고려하여 IP 마킹 서버에 금융거래 프로토콜 맞춤형 정보를 추가로 저장할 경우, 금융 전산망 침해사고 발생할 시 효율적으로 사고 분석과 대처가 가능하고 다양한 금융 부정행위를 탐지할 수 있을 것으로 기대된다.

4. 마킹 서버 추가 기법에 대한 실험 및 검증

이번 장에서는 금융네트워크에서 역추적을 위해 새로운 인프라를 적용하는 방법을 실험적으로 검증해보고자 한다. 먼저 실험환경에 대해 설명하고 실험결과를 통해 본 논문에서 제안하는 방법과 기존의 기법을 비교 분석했다.

4.1 실험 환경

금융 네트워크 모델을 구축하고 역추적 기법을 적용하여 성능을 비교하기 위해 시간 경과에 따른 프로세스와 시스템의 동작을 설계, 분석할 수 있고 네트워크 구성 요소와 패킷의 흐름을 재현할 수 있는 Arena Simulation을 활용했다[1, 6].

역추적 기법 비교를 위해 실험에 사용된 각 Arena 모델을 구성하는 라우터와 노드의 수는 동일하며 사용되는 패킷 또한 같다. 실험에 사용된 패킷은 MIT대학교의 링컨 연구실과 DARPA 침입탐지 평가 그룹에서 개발한 네트워크 침입 탐지 테스트용 dataset 1999를 활용했다. 위 dataset은 공격이 포함된 패킷과 공격이 포함되지 않은 패킷으로 구성되어 있어 여러 상황에서 역추적 기법을 실험하기 용이하며 공공 데이터이기 때문에 누구나 활용하여 역추적 기법의 성능을 비교할 수 있기 때문에 선택하였다[3].

네트워크 구성의 경우, 라우터를 기준으로 Inside와 Outside로 구분되어 있으며 각각의 IP 주소를 할당했다. 금융 전산망 인터넷 연결 구간에 위치한 노드의 경우 192.168.1.90으로 할당했다.

4.2 실험 방법

실험은 Arena Simulation을 활용하여 <Figure 2>와 같은 금융 전산망을 일반화한 네트워크를 구성하고, 기존의 역추적 방법 중 하나인 DFM 방식과 본 논문에서 제안하는 방법을 동일한 패킷과 네트워크 구성에 적용하여 네트워크 측면에서의 효율을 비교하는 방식으로 진행했다.

Outside 1~Outside 6, Inside 1~Inside 3에 해당하는 각 노드들은 Arena Simulation에서 사용하기 위해 전처리된 패킷으로 서로 통신을 하며 하나의 라우터에서 마킹을 수행한다.

4.3 실험 결과

<Table 1>는 Arena Simulation을 활용하여 DFM 역추적 방식과 본 논문에서 제안하는 역추적 방식을 금융 네트워크에 적용한 실험의 결과를 비교 정리하였다. Number out은 네트워크에서 이동되는 패킷의 수를 의미하고 있다. 그러므로 제안하는 방법에서는 최종 목적지가 금융망을 대상으로 하는 패킷을 인프라로 추가 전송하기 때문에 더 많은 수치를 나타낸다. Total Time은 시뮬레이션이 진행되는 시간을 의미하고 WIP(Work In Process)은 진행 중인 작업을 의미한다. Queue Waiting Time은 패킷의 Flow마다 마킹을 하기 위해 소요되는 시간을 뜻한다. Total Time과 WIP, Queue Waiting Time은 제안하는 방법에서 낮은 수치를 나타내고 있는데 이는 역추적에 필요한 프로세스를 네트워크 성능에 영향을 주지 않는 인프라에서 담당하기 때문이다.

결과적으로 실험을 통해 오버헤드는 1% 정도 증가했지만 시간이 3.5% 줄고 라우터가 감당하는 프로세스의 경우도 57% 부담이 줄었다는 것을 확인할 수 있다. 이런 수치를 통해 본 논문에서 제안하는 방법이 금융 전산망에 적합할 있다고 할 수 있다.

〈Table 1〉 Arena Simulation Report

	DFM	Marking Server
Number out	3,300	3,332
Total Time	1,716.00	1,655.50
WIP	33.1434	14.0894
Queue Waiting Time	33.39	0

References

[1] Arena Simulation Software, https://www.arenasimulation.com/.

[2] Belenky, A. and Ansari, N., “IP traceback with deterministic packet marking,” IEEE communications letters, Vol. 7, No. 4, pp. 162-164, 2003.

[3] DARPA 1999 Intrusion Detection Data Sets, https://ll.mit.edu/ideval/data/.

[4] Foroushani, V. A. and Zincir-Heywood, A. N., “Deterministic and authenticated flow marking for IP traceback,” Advanced Information Networking and Applications (AINA), 2013 IEEE 27th International Conference on. IEEE, 2013.

[5] Incident Response Team and Incident

countermeasure planning team of Financial Security Institute, “Effective response to the financial crisis,” 2015.

[6] Kuhl et al., “Cyber attack modeling and simulation for network security analysis,” Proceedings of the 39th Conference on Winter Simulation: 40 years! The best is yet to come, IEEE Press, 2007.

[7] Park, E. Y. and Yoon, J. W., “A study of accident prevention effect through anomaly analysis in E-banking,” The Journal of Society for e-Business Studies, Vol. 19, No. 4, pp. 119-134, 2014.

[8] Savage, S., Wetherall, D., Karlin, a., and Anderson, T., “Network support for IP traceback,” IEEE/ACM Transaction on Networking, Vol. 9, No. 3, pp. 226-237, 2001.

[9] Savage, S., Wetherall, D., Karlin, a., and Anderson, T., “Practical network support for IP traceback,” ACM SIGCOMM Computer Communication Review, Vol. 30, No. 4, pp. 295-306, 2000.

[10] Song, D. X. and Perrig, A., “Advanced and authenticated marking schemes for IP traceback,” INFOCOM 2001, Twentieth Annual Joint Conference of the IEEE Computer and Communications Societies, Proceedings, IEEE, Vol. 2, pp. 878-886, 2001.

저 자 소 개

박근호 (E-mail: happyrjsgh19@gmail.com)
2016년 아주대학교 컴퓨터공학과 졸업
2016년～현재 아주대학교 컴퓨터공학과 석사과정
관심분야 정보보안, 네트워크 보안

최규원 (E-mail: kchoi@ece.iit.edu)
1993년～1996년 KT연구센터 연구원
1998년～1999년 Scientific Research Corp 연구원
1999년～2000년 Broadcom 연구원
2002년 Georgia Institute of Technology 전자컴퓨터공학부 (박사)
2002년～2005년 삼성전자 LSI 책임연구원
2005년～2007년 Sequence Design Inc. 책임연구원
2007년～현재 Illinois Institute of Technology 전자컴퓨터공학부 교수
관심분야 디지털 시스템 설계, 저전력 RFID 시스템 설계

손태식 (E-mail: tsshon@ajou.ac.kr)
2000년 아주대학교 정보및컴퓨터공학부 졸업 (학사)
2002년 아주대학교 정보통신전문대학원 졸업 (석사)
2005년 고려대학교 정보보호대학원 졸업 (박사)
2004년～2005년 University of Minnesota 방문연구원
2005년～2011년 삼성전자 통신/DMC 연구소 책임연구원
2011년～현재 아주대학교 정보통신대학 사이버보안학과 부교수
2017년～현재 Illinois Institute of Technology 방문교수
관심분야 산업제어시스템 보안, 비정상행위탐지, 디지털 포렌식