사물인터넷융복합논문지 Vol. 8, No. 5, pp. 111-117, 2022 https://doi.org/10.20465/KIOTS.2022.8.5.111

Tor 사용자 추적 기술 동향에 관한 연구

한경현[1], 황성운[2*]
[1]홍익대학교 전자전산공학과 학생, [2]가천대학교 컴퓨터공학과 교수

A Research on User Tracing Technologies in Tor

KyungHyun Han[1], Seong Oun Hwang[2*]
[1]Student, Department of Electronics and Computer Engineering, Hongik University
[2]Professor, Department of Computer Engineering, Gachon University

요 약 익명 네트워크는 감시나 트래픽 추적을 피하기 위한 정보통신 보호를 목적으로 설계된 네트워크이다. 그러나 최근에는 이러한 특성을 악용하여 사이버 범죄자들이 익명 네트워크를 활용하여 사이버 범죄를 일으키고, 사법 당국의 추적을 회피하고 있다. 본 논문에서는 익명 네트워크 중 하나인 Tor를 중심으로 관련 연구를 조사한다. 본 논문은 Tor가 어떻게 익명성을 제공하는지 소개하고, Tor를 대상으로 어떻게 사용자를 추적할 수 있는지 소개한다. 또한 각 추적 기술을 비교 분석하였으며, 연구자가 실험 환경을 어떻게 구축할 수 있는지 설명한다.

주제어 : 익명 네트워크, 토르, 추적 기술, 실험 환경 구축

Abstract Anonymous networks are designed to protect information and communication by avoiding monitoring or tracking traffic. In recent years, however, cybercriminals have evaded law enforcement tracking by exploiting the characteristics of anonymous networks. In this paper, we investigate related research focusing on Tor, one of the anonymous networks. This paper introduces how Tor provides anonymity, and how tracing technologies can track users against Tor. In addition, we compare and analyze tracing techniques, and explain how a researcher can establish an experimental environment.

Key Words : Anonymous Networks, Tor, Tracing Technology

1. 소개

익명 네트워크는 감시나 트래픽 추적을 피하기 위한 정보통신 보호를 목적으로 설계된 네트워크이다. 일반적인 네트워크에서 노출되는 출발지 IP와 도착지 IP가 사용자 또는 서버의 IP인 것에 비해, 익명 네트워크는 패킷 전달 과정에서 출발지 IP와 도착지 IP를 숨기면서 목적지까지 전달한다. 그러나 최근에는 이러한 특성을 악용하여 사이버 범죄자들이 익명 네트워크를 활용하여 사이버 범죄를 일으키고, 추적을 회피하고 있다. 특히, 토르에서는 납치, 신분증 위조, 아동 포르노, 마약 거래 등 중범죄와 이와 관련된 거래가 연간 1,000억 원에 달한다는 조사 결과가 있을 정도로 그 규모가 상당하다[1].

최근 마이크로 보일러[2], 스마트 휴지통[3], 청년 지원사업[4] 등 IoT 기반 서비스가 많아지고 있다. IoT 기기와 이와 동시에 IoT 사용자의 프라이버시 침해 우려가 커지고 있다. 이를 방지하기 위해 IoT 환경에서 프라이버시 보호를 위해 익명 네트워크를 사용하는 방안이 연구되었다[5]. 익명 네트워크 중 하나인 Tor에서도 IoT의 프라이버시 보호를 지원하기 위해 Home Assistant 프로젝트를 진행하고 있다[6]. 이는 반대로 IoT 시스템 내부에 공격자가 있는 경우 공격자의 프라이버시가 보호되

이 논문은 2022년 정부(방위사업청)의 재원으로 국방과학연구소의 지원을 받아 수행된 연구임(UI220040XD)
*교신저자 : 황성운(sohwang@gachon.ac.kr)
접수일 2022년 7월 25일 수정일 2022년 9월 18일 심사완료일 2022년 9월 22일

어 추적할 수 없음을 의미한다. 따라서 필요한 경우 관리자는 공격 패킷을 추적할 수 있어야 한다.

본 논문은 다음과 같이 구성된다. 2장에서는 Tor에 관해 설명한다. 3장에서는 익명 네트워크의 추적 기술을 소개하고, 4장에서는 실험을 위한 방법을 소개한다. 5장에서는 본 조사 연구의 결론을 정리한다.

2. 관련 연구

2.1 익명 네트워크 추적 기술에 대한 기존 조사

[7]는 익명 네트워크를 폭넓게 조사, 분석하고 있다. [7]는 익명 네트워크를 지연 시간에 따라 저지연과 고지연으로 구별하였으며, 사용자 추적 공격에 대해서도 어플리케이션 기반 공격과 네트워크 레벨 공격으로 구별하여 소개한다.

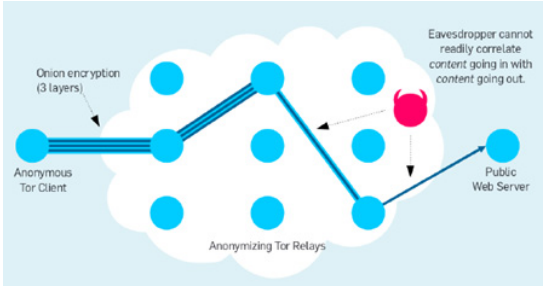
먼저 익명 네트워크는 Tor를 대상으로 하여 조사하였다. Tor는 저지연 익명 네트워크 중 하나로 전 세계에 다수의 사용자가 있는 대표적인 익명 네트워크이다. 공격 기술에서는 사용자/개발자 부주의로 발생하는 어플리케이션 기반 공격은 제외하고, 순수하게 익명 네트워크의 약점을 찾아 공격하는 네트워크 레벨 사용자 추적 기술을 위주로 조사하였다.

2.1 Tor 소개

Tor는 어니언 라우팅(Onion Routing)을 이용하여 출발지와 목적지의 IP를 노출하지 않아 사용자에게 익명성을 제공하는 기술이다.

2.2 Tor의 작동 원리

아래 그림 1과 같이 Tor의 어니언 라우팅은 출발지에서 목적지로 패킷을 직접 전달하지 않고, 최소 3개의 Tor 릴레이 노드를 거쳐 전달한다. Tor 내에서 패킷은 IP를 포함하여 모두 암호화되며, 이 암호화는 릴레이 노드 수만큼 겹겹이 암호화되어 각 릴레이 노드에서 복호화하더라도 오직 '다음 노드의 IP'만 공개된다. 먼저 사용자가 Tor를 통해 3개의 릴레이 노드를 배정받고 그들의 공개키를 받아서 패킷을 암호화하고 첫 번째 노드인 Entry Node의 IP만 공개하여 전송한다. Entry Node는 패킷을 복호화하여 다음 노드인 Middle Node의 IP를 확인하고 패킷을 전달한다. Middle Node도 같은 방식으로 마지막 노드인 Exit Node에 패킷을 전달하며, Exit Node도 같은 방식으로 다음 노드 IP(목적지 IP)를 확인하여 전달한다.



[Fig. 1] How does onion routing work?

정리하면, Entry Node는 출발지 IP를 알 수 있지만, 목적지 IP를 알 수 없다. Exit Node는 목적지 IP는 알 수 있지만, 출발지 IP를 알 수 없다. Tor의 릴레이 노드는 패킷을 전달만 할 뿐 자신이 Entry/Exit Node인지 구별하지 못하며, 서로 정보를 교환하지도 않는다. 그리고 외부에서 릴레이 노드가 전달하는 패킷을 도청하더라도 중간 단계에서 패킷은 모두 겹겹이 암호화 되어 비교 매칭이 어렵다.

2.3 Tor 히든 서비스

위와 같이 Tor를 이용하면 사용자의 IP는 익명성을 보장받을 수 있다. 하지만 서버의 경우 사용자가 접속할 수 있도록 IP를 공개해야 한다. 이를 위해, Tor는 히든 서비스를 제공한다. Tor를 사용하는 서버는 위 어니언 라우팅으로 릴레이 노드와 연결되어 있으며 자신의 서버 IP 대신 릴레이 노드의 IP를 공개한다. 사용자는 모두 릴레이 노드의 IP를 통해 접속을 시도하며, 서버의 IP는 어니언 라우팅을 통해 보호된다. 특히, 사용자 측과 서버 측에서 각각 어니언 라우팅을 사용할 수 있으므로 양측이 동시에 익명성을 보장받을 수 있다.

3. 익명 네트워크의 추적 기술

추적 기술은 어플리케이션 기반 공격과 네트워크 레벨 공격으로 분류된다. 어플리케이션 기반 공격은 익명 오버레이 네트워크를 이용하는 응용프로그램에 의해 발생되는 공격으로, 주로 사용자 또는 개발자의 부주의로 IP가 노출된다. 예를 들어, 웹 응용프로그램에서 사용자 IP를 기록한다면, 익명 오버레이 네트워크를 사용하더라도

사용자의 IP가 노출될 수 있다. 네트워크 레벨 공격은 익명 오버레이 네트워크가 제공하는 익명성에 대한 직접적인 공격으로, 주로 익명 오버레이 네트워크가 성능을 위해 익명성을 희생하면서 IP를 노출할 수 있는 취약점을 이용한다. 대부분의 저지연 시스템은 성능과 익명성에 대한 상충(trade-off) 관계로 인해 일정 부분 익명성을 희생하기 때문에 이러한 점을 노리는 추적 기술이 연구되고 있다.

3.1 Timing Attack

Timing Attack은 네트워크에 흐르는 패킷의 시간 간격을 통해 사용자를 식별하는 추적 기술이다. 이 공격은 수많은 익명 오버레이 네트워크 사용자 중에서 추적 대상 하나를 골라내는 공격이 아니라, 피해 서버와 통신한 것으로 추정되는 사용자가 실제로 통신했는지를 검증하는 용도로 활용되는 추적 기술이다. Timing Attack은 아래와 같이 패시브/액티브/하이브리드의 3가지로 분류된다.

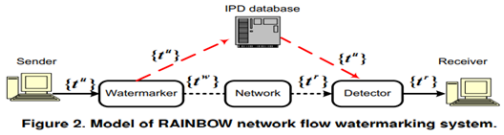
〈Table 1〉 Classification of Timing Attack

Passive	The attacker stores the timing patterns of the victim's traffic flow at one communication end.
Active	The attacker makes modifications in the timing patterns of the victim's traffic flow at one communication end to mark the flow.
Hybrid	In this scheme, the attacker stores the timing information as well as make modifications to the network flow.

Timing Attack은 분석 대상이 될 두 사용자가 미리 정해져 있어야 하며, 익명 오버레이 네트워크가 임의의 네트워크 지연을 발생하거나 경로를 자주 수정하면 공격이 실패하는 단점이 있다.

3.1.1 Rainbow

Rainbow[8]는 패킷 간 딜레이(IPD: Inter-Packet Delay)를 이용하는 하이브리드 Timing Attack이다. 이는 대부분의 추적 기술 연구에서 사용하는 가정인 Entry와 Exit 노드를 제어할 수 있다는 전제로 연구되었다. 그림 2와 같이 Entry 노드에 Watermarker 기능을 추가하고, Exit 노드에 Detector 기능을 추가한다. Watermarker는 각 송신자에 대해 특정 IPD 간격으로 패킷을 전달하며, 이 특정 IPD를 IPD database에 저장한다. Detector는 수신되는 패킷이 특정 수신자에게 전달되는지 확인하고, 그 패킷이 수신되는 간격을 분석하여 IPD database에 등록된 IPD와 대조한다. 이러한 방식으로 공격자는 송신자와 수신자 간에 통신이 있음을 검증할 수 있다.

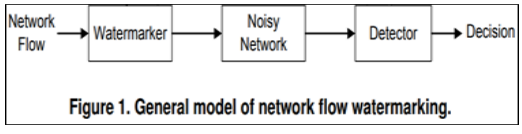


[Fig. 2] Structure of Rainbow System

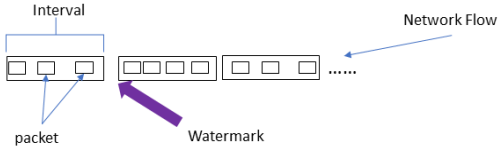
이 공격은 Watermarker가 기존의 다른 공격 기법에 비해 상대적으로 작은 네트워크 지연을 추가하여 추적 공격의 은닉성을 향상시킨다. 단, 분석 대상이 많아지면 저장해야 하는 Watermark(IPD)도 많아지기 때문에 대규모 분석에 활용하기 힘들다는 단점이 있다.

3.1.2 SWIRL

SWIRL[9]는 interval(패킷의 그룹) 간 딜레이를 이용하는 액티브 Timing Attack이다. 이 연구도 Rainbow와 동일하게 Entry와 Exit 노드를 제어할 수 있다는 전제로 연구되었으며, 그림 3과 같이 Entry 노드에 Watermarker 기능을 추가하고, Exit 노드에 Detector 기능을 추가한다. Rainbow와의 차이점은 이 논문에서 watermark는 패킷 간 딜레이인 IPD를 사용하는 것이 아니라, 그림 4와 같이 패킷들을 interval이라는 그룹으로 묶고 interval 간 딜레이를 watermark로 사용한다는 점이다.



[Fig. 3] Structure of SWIRL System



[Fig. 4] Watermark in SWIRL System

이 공격은 IPD를 활용하지 않고 패킷을 interval로 묶었기 때문에 일부 패킷이 지연, 손실되더라도 추적이 가능하다는 장점이 있다. 단, 이 기법은 다양한 파라미터

를 통해 interval을 생성하기 때문에 성능과 공격 성공률 사이의 상충 관계가 있어 최적의 파라미터를 선택하여 분석하기 어렵다는 단점이 있다.

3.1.3 Timing Attack 비교 분석

두 Timing Attack들의 장점을 비교하면 아래 표 2와 같다. 두 기법 모두 패킷 흐름에 추가되는 지연이 매우 작아서 은닉성이 높다. 그중 Rainbow는 대규모 분석은 힘들지만 설정해야 하는 파라미터가 적다. 반대로 SWIRL은 패킷을 묶어서 분석하므로 더 많은 패킷을 분석할 수 있으나 파라미터 설정이 어려운 단점이 있다.

〈Table 2〉 Comparison of Timing Attack

	Rainbow	SWIRL
Communication delay	Low	Low
Concealment	High	High
Tracking ability	Medium	High
Parameter setting difficulty	Easy	Hard
large-scale analysis	Hard	Medium

3.2 Multiplication Attack

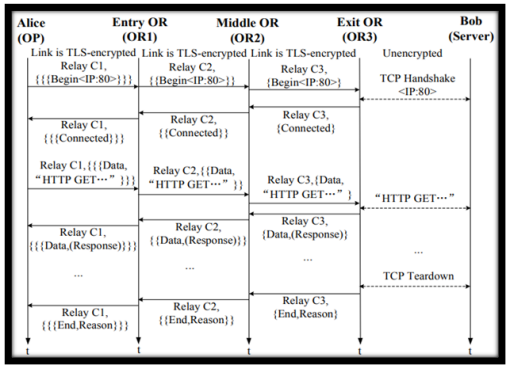
Multiplication Attack은 네트워크에 흐르는 패킷의 일부분을 변경하여 변경된 부분에 관련된 응답을 하는 사용자를 식별하는 추적 기술이다. 이 공격은 수많은 익명 오버레이 네트워크 사용자 중에서 특정 사용자를 찾아낼 수 있다. Multiplication Attack은 아래와 같이 4가지 연구가 조사되었다.

〈Table 3〉 Classification of Multiplication Attack

Attack Methods	Methods Working
Replay	find the user sending the cell by modifying some data to induce the user to send an additional cell
Injection	add a specific cell and find out who is listening to that cell
Modification	find a user by modifying some cells and detecting the modified part
Deletion	find a user by inducing an error message to be sent by omitting a specific cell

3.2.1 Replay 방식

X Wang[10]이 제안한 replay 방식의 Multiplication Attack은 아래 그림 5과 같이 img 태그를 활용한다. 사용자 Alice가 서버 Bob에 접속하면 서버는 html 파일을 송신하는데, Exit 노드가 이 html 내부에 이미지 태그를 추가한다. html 규칙에 따라 사용자 Alice는 해당 이미지 파일을 얻기 위해 서버에 접속하면서 추가적인 cell을 발생한다. 참고로, 토르 트래픽은 514바이트 cell 단위로 전송된다. 이를 이용하여 Entry 노드에서 추가적인 cell을 보내는 사용자를 추적 대상으로 식별할 수 있다.

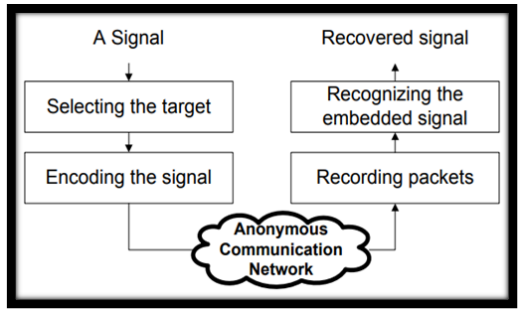


[Fig. 5] Replay Method using Img Tag

단점으로는, 모니터링하는 웹서버뿐만 아니라 다른 일반 웹서버도 이미지를 많이 사용할 수 있으므로 비슷하게 추가 cell을 만드는 다른 사용자를 잘못 탐지할 수도 있다.

3.2.2 Injection 방식

Z Ling[11]이 제안한 injection 방식의 Multiplication Attack은 아래 그림 6과 같이 특정 신호를 포함하는 추가 cell을 활용한다. Exit 노드가 추적하고자 하는 트래픽에 추가 cell을 포함시켜 전달하고, 이 cell을 Entry 노드에서 감지하여 이 cell을 전달받는 사용자를 추적 대상으로 식별할 수 있다.

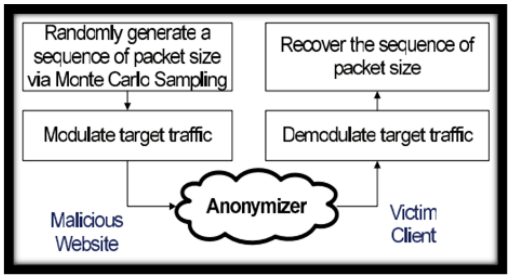


[Fig. 6] Injection Method

이 공격은 cell을 추가하는 것이기 때문에 원래 cell이 적은 트래픽이더라도 공격이 가능하며, 탐지율이 100%에 근접한다는 장점이 있다. 단점으로는, 추가 cell을 삽입할 때 카운트를 바꾸게 되는데, 네트워크 지연이나 익명 오버레이 네트워크의 정책 등으로 카운트가 뒤섞이면 탐지를 못 할 수도 있다.

3.2.3 Modification 방식

Z Ling[12]은 아래 그림 7과 같은 Modification 방식의 Multiplication Attack도 제안하였다. Exit 노드가 추적하고자 하는 트래픽의 첫 부분의 cell을 일부 수정하여 패킷 크기가 특정 sequence가 되도록 패킷을 만든다. Entry 노드는 수신하는 트래픽에 패킷 크기가 특정 sequence인지 확인하여 이 트래픽을 전달받는 사용자를 추적 대상으로 식별할 수 있다.



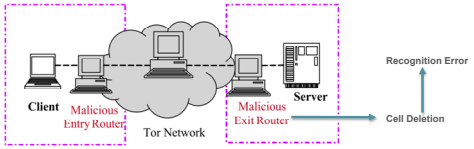
[Fig. 7] Modification Method

이 공격은 cell을 수정하는 것이기 때문에 원래 cell이 적은 트래픽이더라도 공격이 가능하다. 단점으로는, cell을 수정하기 위해 통신이 지연된다는 점이며, 특히 수정된 cell이 이전 cell과 결합되면 해당 sequence를 감지하지 못해 탐지를 못 할 수도 있다.

3.2.4 Deletion 방식

Z Ling[13]이 제안한 Deletion 방식의 Multiplication Attack은 아래 그림 8와 같이 특정 cell을 삭제하여 사용자를 탐지한다. Tor 네트워크에서는 CELL_RELAY_DATA라는 cell이 있는데, 이 cell이 삭제되면 인식 오류가 발생하여 오류를 정정하기 위한 패킷이 생성된다. 이 패킷에 client IP가 포함되어 있는데, 이를 통해 사용자를 식별할 수 있다.

Cell 인식 오류로 추가 패킷을 생성하는 것은 Tor relay가 자동으로 진행하기 때문에, cell을 삭제할 용도로 Entry나 Exit 노드 중 하나만 제어해도 공격이 성공할 수 있다는 장점이 있다. 단점으로는, Entry 노드가 아닌 중간 노드에서 cell 오류를 감지하면, 중간 노드는 직접 사용자와 통신하지 않으므로 사용자의 IP가 아닌 다른 Tor 노드의 IP를 보내게 된다는 점이다.



[Fig. 8] Deletion Method

3.2.5 Multiplication Attack 비교 분석

위 Multiplication Attack들의 장점을 비교하면 아래 표 4와 같다. 4번 기법은 Entry와 Exit 노드 중 하나만 제어해도 공격할 수 있으므로 실용성(effectiveness)이 높다. 하지만 중간 노드에서 cell 오류를 감지할 수 있다는 점에 의해 False positive rate가 상대적으로 높다. 2번과 3번 기법은 공격으로 인해 발생하는 패킷의 양이 매우 적기 때문에 공격이 사용자에게 노출될 확률이 낮고, 공격자가 만든 값을 감지하기 때문에 정확도가 비교적 높다.

〈Table 4〉 Comparison of Multiplication Attack

	Replay	Injection	Modification	Deletion
Effectiveness	High	High	High	Medium
Packets Required	Higher	Less	Less	Higher
Attack Detectability	Medium	Low	Low	Medium
Control of Entry and Exit OR	Both	Both	Both	One
False Positive Rate	Medium	Low	Low	High

4. 익명 네트워크의 추적 기술 실험 방법

4.1 실험 방법

이와 같은 익명 네트워크 추적 기술 연구를 진행하기 위해서는 실험 환경을 구축할 수 있어야 한다. 익명 오버레이 네트워크 중 하나인 Tor를 기준으로 실험 환경 구축 방법을 조사하였다. 크게 1) 시뮬레이터를 사용하는 방법, 2) Tor 릴레이 노드를 제어하는 방법, 3) 사용자와 Tor 사이에 특정 제어기를 설치하는 방법으로 나뉜다.

4.1.1 시뮬레이터 사용

Tor와 같은 대규모 네트워크는 직접 구축하기 어렵기 때문에 시뮬레이션을 고려할 수 있다. Shadow[14]는 가장 현실적으로 사설 네트워크를 구축하고 수천 개의 연결이 있는 시스템을 시뮬레이션 할 수 있으며, 각 노드에서 임의의 코드를 직접 실행할 수도 있는 네트워크 시뮬레이터이다. 네트워크 프로토콜이나 라우팅 특성까지 설정할 수 있다.

하지만 시뮬레이션을 위해서는 대량의 컴퓨팅 리소스를 준비해야 하는 단점이 있다. Torproject[15]를 참고하면 Tor에는 6천여 개의 릴레이 노드와 80만 개의 동시 사용자가 있다. 이 규모의 시뮬레이션을 위해서는 4TB 정도의 RAM이 필요하다.

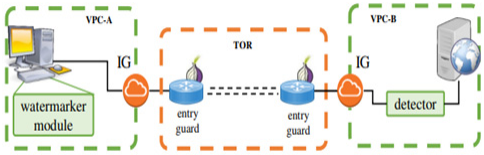
4.1.2 Tor 릴레이 노드 제어

Tor 네트워크를 직접 사용하는 것도 고려할 수 있다. 이 방법은 Tor 네트워크에 구축된 릴레이 노드 일부를 제어하여 실제 환경에서 실험하는 것이다.

하지만 이는 Tor 네트워크의 장애를 유발할 수 있으므로 Tor 운영자에 의해 철저하게 관리되고 있다. 이 방법으로 실험하기 위해서는 Tor 위원회에 실험 방법/리스크/이점 등을 모두 설명해야 하며 Tor 연구 지침을 엄격하게 따라야 하고, 불이행 시 네트워크 사용에 있어서 제재를 당하게 된다.

4.1.3 사용자와 Tor 사이에 제어기 설치

이 방법은 아래 그림 9와 같이 사용자가 Tor와 직접 연결되지 않고, 중간에서 자체 설계된 제어기를 통해 접속하도록 하는 방법이다. 제어기가 실제 Tor 네트워크의 릴레이 노드에 설치된 것은 아니지만 사용자/서버의 관점으로는 제어기가 릴레이 노드에 설치된 것과 크게 다르지 않다. 사용자가 전달한 패킷은 실제로는 제어기를 통해 Tor 네트워크에 들어가서 릴레이 노드에 전달되지만, Tor 네트워크의 릴레이 노드에 전달된 후 제어기가 동작했다고 봐도 문제없다.



[Fig. 9] A Model with a Controller Installed between the User and Tor

앞의 두 방법은 현실적으로 수행하기 어려운 면이 있으므로, 많은 논문에서는 이 방법을 주로 사용한다. Tor 네트워크 관점에서는 제어기가 사용자로 인식되므로 Tor 네트워크를 단순히 사용할 뿐이라서 Tor 위원회에 알리거나 Tor 연구 지침을 따를 필요가 없다. 또한 실제 Tor 네트워크를 이용하면 연구자가 제어하는 Entry/Exit 노드가 실제로 선택될지는 확률적이지만 이 방법은 항상 자체 설계한 제어기를 통해 Tor 네트워크에 진입하므로 Entry/Exit 노드가 항상 선택된다고 볼 수 있다.

하지만 Tor 릴레이 노드를 직접 제어하는 것은 아니기 때문에 릴레이 노드 사이의 패킷 전달이나 캡처 등 일부는 제어할 수 없다는 단점이 있다.

5. 결론

본 논문은 Tor와 관련된 추적 기술 연구들을 기초 지식, 관련 기술, 핵심 아이디어, 장단점을 포함한 다각적인 관점에서 분석하고 비교했다. 또한 추적 기술 관련 연구를 진행하기 위해 필수적인 실험 환경 구축 방법들을 조사하고 비교했다.

본 연구를 바탕으로 연구자가 익명 네트워크와 관련 추적 기술을 쉽게 이해하고, 기존 연구에 사용된 트래픽 특성을 분석해 볼 수 있다. 최근 인공지능이 많이 발전하였으므로 이를 이용하여 더 다양한 트래픽 특성을 분석하여 각 노드에서 전달되는 패킷을 매칭시키는 연구가 필요하다.

REFERENCES

[1] Norwich University Online, Deep Web Crime Requires New Forensic Approaches[Internet], https://online.norwich.edu/academic-programs/resources/deep-web-crime-requires-new-forensic-approaches

[2] S. C. Jang, “Basic Study on the IoT Micro Boiler,” Journal of Internet of Things and Convergence, Vol.8, No.1, pp.23-29, 2022.

[3] T. K. Kim, “IoT (Internet of Things)-based Smart Trash Can,” Journal of Internet of Things and Convergence, Vol.6, No.1, pp.17-22, 2020.

[4] S. Lee and K. Cho, “Seeking an Approach to Youth Job Search Allowance Support Project using IoT in the Untact Era,” Journal of Internet of Things and Convergence, Vol.6, No.3, pp.21-30, 2020.

[5] I. G. Han, J. H. Yeon, H. Y. Lee and H. J. Kim, “Concept of a Layer for Privacy Protection of Upstream Communications in IoT Environments,” In Proceedings of the Korea Information Processing Society Conference, pp. 468-469, 2019.

[6] Tor Network Reachs Internet of Things[Internet], https://www.hwlibre.com/ko/la-red-tor-llega-al-internet-las-cosas/

[7] E. Erdin, C. Zachor and M. H. Gunes, "How to find hidden users: A survey of attacks on anonymity networks," IEEE Communications Surveys & Tutorials, Vol.17, No.4, pp.2296-2316, 2015.

[8] A. Houmansadr, N. Kiyavash and N. Borisov, "Non-Blind Watermarking of Network Flows," IEEE/ACM Transactions on Networking, Vol.22, No.4, pp.1232-1244, 2013.

[9] A. Houmansadr and N. Borisov, "SWIRL: A Scalable Watermark to Detect Correlated Network Flows," In NDSS, 2011.

[10] X. Wang, J. Luo, M. Yang and Z. Ling, "A novel flow multiplication attack against Tor,"?In 2009 13th International Conference on Computer Supported Cooperative Work in Design, Santiago, pp.686-691, 2009, Dissertations.

[11] Z. Ling, J. Luo, W. Yu, X. Fu, D. Xuan and W. Jia, "A New Cell-Counting-Based Attack Against Tor," in IEEE/ACM Transactions on Networking, Vol.20, No.4, pp.1245-1261, 2012.

[12] Z. Ling, X. Fu, W. Jia, W. Yu and D. Xuan, “Novel packet size based covert channel attack against anonymizer," IEEE Transactions on Computers, Vol.62, pp. 186-190, 2013.

[13] Z. Ling, J. Luo, W. Yu, X. Fu, W. Jia and W. Zhao, "Protocol-level attacks against Tor," Computer Networks, Vol.57, No.4, pp.869-886, 2013.

[14] K. Kiran, S. Saurabh, M. Usman, P. D. Shenoy and K. R. Venugopal, "Anonymity and performance analysis of stream isolation in tor network," In 2019 10th International Conference on Computing, Communication and Networking Technologies (ICCCNT) pp.1-6, 2019.

[15] Rob Jansen, New Foundations for Tor Network Experimentation[Internet], https://blog.torproject.org/new-foundations-tor-network-experimentation/

한 경 현(KyungHyun Han) [정회원]

- 2015년 2월 : 홍익대학교 컴퓨터정보통신학과(공학학사)
- 2017년 2월 : 홍익대학교 일반대학원 전자전산공학과 (공학석사)
- 2017년 3월 ~ 현재 : 홍익대학교 일반대학원 전자전산공학과 (공학박사과정)

〈관심분야〉
사이버보안

황 성 운(Seong Oun Hwang) [정회원]

- 1993년 8월 : 서울대학교 수학과 (이학사)
- 1998년 2월 : 포항공과대학교대학원 정보통신학과 (공학석사)
- 2004년 8월 : 한국과학기술원 전자전산학과 (공학박사)
- 2006년 1월 ~ 2006년 12월 : University of Michigan 박사 후 연구원
- 2008년 3월 ~ 2020년 2월 : 홍익대학교 컴퓨터공학과 교수
- 2020년 3월 ~ 현재 : 가천대학교 컴퓨터공학과 교수

〈관심분야〉
정보보호, 사이버보안, 기계학습