Mix-Net을 이용한 영상 데이터 전송 시 송수신자의 익명성 기술에 관한 연구 동향

송유성°, 변진욱, 이동훈
고려대학교 정보보호대학원

The Trend of Study for Anonimity of Sender and Reciever through the Mix-Net

Yu-Seong Song°, Jin-Wook Byun, Dong Hoon Lee
Graduate School of Information Security, Korea University

요 약

멀티미디어 기술의 급격한 발전으로 인해 대부분의 전송되는 파일들은 다양한 멀티미디어 데이터를 포함하고 있다. 이러한 멀티미디어 데이터를 전송할 때 송수신자의 익명성 보장은 최근 PET 기술의 급격한 관심과 더불어 상당히 큰 이슈로 부각되고 있다. 그러므로 송수신자의 익명성을 보장하는 기술들에 관한 최근 연구 동향을 살펴보는 일은 중요하다. 본 논문에서는 다양한 멀티미디어 데이터를 전송 시 송수신자의 익명성을 보장하는 최근 기술 및 현황들을 Mix-net 기술을 중심으로 살펴본다.

1. 서론

1980년대 중반부터 "Privacy enhanced mail Privacy" [1] 이란 용어의 사용으로 인해 메시지의 전송 보안 차원의 보안이라는 좁은 범위의 개인 정보보호에 관심을 가지기 시작했다. 그 이후 인터넷의 발달로 인해 인터넷 보안과 관련된 기술에 관심을 가짐으로써 온라인상에서의 Privacy 보호 기술과 관련 정책 수립에 각 국에서 노력이 가해졌다. 하지만, 정보통신의 급격한 발달로 인해 Privacy 보호 기술과 관계 정책이 이를 따라가지 못하고 있는 실정이다.

PET(Privacy Enhanced Technologies)는 신원 확인이 가능한 데이터 수집을 최소화하거나 하지 못하도록 함으로써 개인의 Privacy를 보호하는 다양한 기술들을 말한다. PET를 통해서 보장해야 할 성질들을 정리하면 다음과 같다.

① **익명성(Anonymity)** : 사용자가 자신의 신분을 드러내지 않고 서비스나 리소스의 사용을 보장하는 것을 의미한다.

② **비관찰성(Unobservability)**. 이것은 사용자가 이용하는 서비스나 리소스를 다른 사람이 관찰할 수 없게 하는 성질을 의미한다.

③ **비연결성(Unlinkability)**. 비연결성(Unlinkability)은 사용자들이 리소스나 서비스를 이용할 때 다른 사용자들이 이를 서로 링크하지 못하게 하는 성질을 의미한다 [2].

③ **가명성(Pseudonimity)**. 가명성(Pseudonymity)은 사용자가 그의 신분을 드러내지 않고 서비스나 리소스를 이용할 수 있게 해 준다. 특히 사용자가 그의 행위에 책임을 져야 하며 익명성을 제공받지 못할 경우에 고려해야 할 성질이다.

멀티미디어 기술의 급격한 발전으로 인해 대부분의 전송되는 파일들은 다양한 멀티미디어 데이터를 포함하고 있다. 이러한 멀티미디어 데이터를 전송할 때 송수신자의 익명성 보장은 최근 PET 기술의 급격한 관심과 더불어 상당히 큰 이슈로 부각되고 있다. 그러므

로 송수신자의 익명성을 보장하는 최근 연구 동향을 살펴보는 일은 중요하다.

기본적으로 익명성(Anonymity)을 제공하는 잘 알려진 기술들은 크게 함축적 주소와 브로드캐스팅(Implicit Addresses and Broadcasting) [3, 4], DC-Networks [1], 그리고 Mixes [5] 가 있다. 이 중 ad-hoc 환경에 적합하며 현재 가장 많이 이용되고 있는 구조가 Mix들을 이용한 Mix-nets이다. 영상 매체의 발달로 인해 많은 영상 데이터들이 무방비 상태로 네트워크 상에서 전송되고 있다. 이 같은 영상 데이터들이 전달 될 때 송수신자와 익명성을 보장하면서 전송될 수 있게 도와주는 기술이 Chaum이 최초로 제안한 Mix-Net의 개념이다 [5].

본 논문에서는 Mix-Nets의 기술 개념과 이러한 Mix-net의 공격 형태 그리고 최근에 연구되고 있는 Hybrid Mix-nets의 연구 동향을 분석한다.

2. Mix-Nets [5]

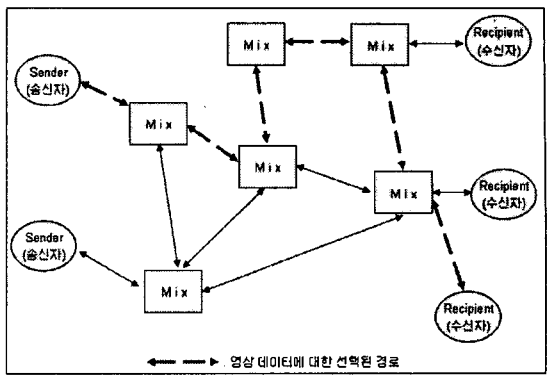
개인 통신 채널은 구성원 간의 익명 통신을 위해 사용된다. 익명성을 제공하는 기본 기술 중 최근 이슈가 되고 있는 것이 Mix-Nets이다. 최초로 Chaum에 의해 제안된 Mix-Nets의 개념은 송·수신자 사이에 Mix라는 서버를 둠으로써 송·수신자간의 관계 및 연결성을 숨기는 Network 환경을 의미한다 [5].

Mix는 특별한 네트워크 스테이션으로써, 메시지를 모아 저장하며, 들어오는 암호문 리스트를 복호화하여 랜덤한 순서로 출력하는 역할을 한다. 즉, 입력과 출력 값의 관계를 숨김으로써 프라이버시(Privacy)를 요구하는 많은 응용분야에 적용이 가능하다.

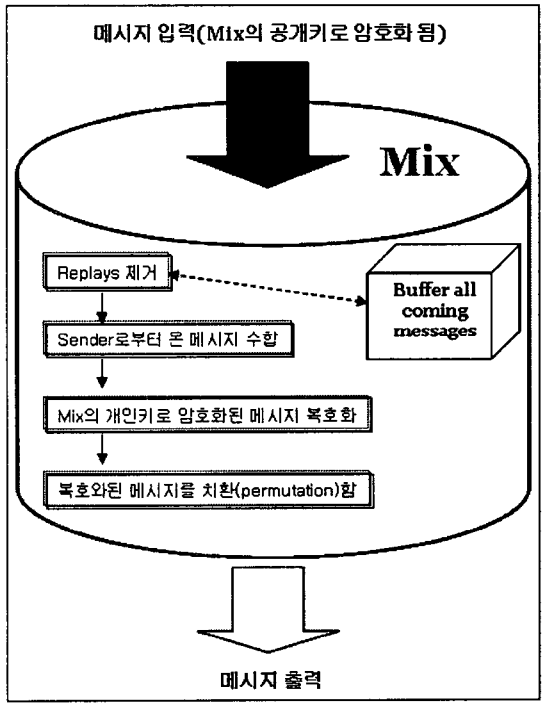
적어도 하나의 Mix를 신뢰할 수 있어야 안전한 Mix-Nets의 구성이 가능하다. Mix-Nets에서 송신자의 익명성(Anonymity)는 Mix로 들어가는 값에 랜덤 스트링(random string)을 삽입함으로써 제공되어지며, 수신자의 익명성은 함축적 주소(Implicit Addresses)와 브로드캐스팅(Broadcasting)를 함께 사용함으로써 제공 되어진다 [3,4,5]. [그림1]은 기본적인 Mix-Net의 구조를 나타낸 것이고, [그림2]는 Mix 내부의 동작 원리를 나타낸 것이다.

2.1. 공격 유형과 해결책

Mix-Nets에 대한 공격 유형은 크게 수동적 공격



[그림 1] Mix network의 예



[그림 2] Mix의 동작 원리

(Passive Attack)과 적극적 공격(Active Attack)으로 나눌 수 있다. 수동적 공격방법으로는 메시지 크기를 관찰함으로써 이루어지는 공격과 메시지의 도착과 출발 시간을 관찰함으로써 이루어지는 공격으로 나눈다. 앞선 공격을 막기 위해서는 메시지의 크기가 전체 네트워크를 통해서도 항상 일정하게 변치 않게 하는 방법이 있다. 이를 위해 랜덤 데이터(random data)를 지닌 일정한 길이의 패딩 메시지(padding message)를

삽입함으로써 항상 입,출력 데이터의 길이를 일정하게 유지시킨다 [5,6]. MIx로의 메시지 도착과 출발 시간을 비교당하는 공격을 막기 위해서는 배치(batch)와 풀(pool)을 이용해 메시지를 출력함으로써 막을 수 있다 [7].

적극적 공격 방법은 메시지 흐름의 직접적인 변화를 통해 이루지는 공격으로 고립, 신원확인(Isolate & identify) 공격방법과 메시지 반복(Message Replay) 공격방법이 있다. 고립, 신원확인 공격은 Mix가 입력되는 패킷들(packets)이 서로 다른 송신자로부터 왔는지 결정할 수 없을 경우에 공격자가 들어오는 패킷들을 가로채어 각 패킷을 고립시키고, (n-1)개의 자신의 패킷을 함께 보냄으로써 원하는 패킷의 이동경로를 알 수 있는 방법이다. 이를 막기 위해서는 Mix에 배치가 가득 찼을 때 쓰레기 메시지들(dummy messages)을 전송하면 된다 [7].

메시지 반복(Message Replay) 공격은 수신자의 메시지를 추적하기 위해 사용된다. 만약 공격자가 메시지를 포착해서 많은 복사 본을 첫 Mix에 전송한다면, 각 Mix에서 똑같아 보이는 많은 메시지들이 같은 경로를 통해 전달되기 때문에 그 연결성을 쉽게 알 수 있다. 이를 막기 위해 각 Mix는 메시지의 기록을 유지하고 있어야 하며, 일정 시간이 되면 반복되는 메시지들은 버려야 한다. 반복되는 메시지는 ID 로그를 유지함으로써 감지될 수 있다. 하지만, 적극적 공격을 막기 위해 사용되어지는 배치를 이용하는 새로운 공격 또한 이루어졌다. 공격자가 Mix로 들어오는 대부분 또는 모든 메시지들을 지연시키고 버리거나 자신의 메시지들로 배치를 넘치게 함으로써 Mix의 입력 값과 출력 값의 연결성을 깰 수 있다. 이 같은 공격을 혼합공격(blending attack)이라 한다 [7,8].

위와 같은 혼합공격에 대한 취약점들을 막기 위 Mixes 자체의 구성을 바꿀 필요가 있다. 기본적인 Mix의 구성으로는 크게 Mix가 threshold만큼의 메시지로 채워지면 그만큼의 메시지를 출력하는 Threshold Mix와 일정한 주기의 시간마다 메시지를 출력하는 Timed Mix가 있다. 이 두 가지를 결합한 Threshold or Timed Mix 또는 Threshold&Timed Mix가 존재하기도 있다. 이러한 다양한 Mix들의 특징 및 동작과정을 모두 다루는 것은 지면 관계상 생략한다.

Mix를 구성할 때 가장 중요한 것은 메시지의 딜레이를 최소화하고, 익명성을 최대화 하는 데 있다. [표 1]에 여러 Mixes의 구성 형태와 각각의 메시지 딜레이와 익명성을 측정해 비교하였다.

3. Hybrid Mix-Nets

긴 메시지에 대한 효율성을 높이기 위해 공개키 암호와 대칭키 암호를 같이 사용함으로써 새로운 Mix-Net의 개념으로 등장한 것이 Hybrid Mix-Net이다. 최초로 Ohkubo와 Abe[9]가 강건함(Robustness)의 성질과 대칭키 암호의 효율적인 사용을 지닌 Hybrid mix network를 구성하는 것이 가능함을 보였다. 보안적인 측면은 랜덤 오라클 모델(random oracle model)을 이용해 증명된다. 즉, Mix-Net의 익명성을 깨는 것을 대칭키 암호 기술의 일련의 구별 불가능을 깨는

		Delay			Anonymity		
		Avg.	Min.	Max.	Avg.	Min.	Max
Simple	Threshold	$\frac{n}{2r}$	ϵ	∞	n	n	n
	Timed	$\frac{t}{2}$	ϵ	$t-\epsilon$	rt	0	mix capacity
	Threshold or Timed		ϵ	$t-\epsilon$		0	n
	Threshold & Timed		ϵ	∞		n	mix capacity
Constant Pool	Threshold	$\left(1+\frac{f}{n+f}\right)\frac{n}{r}$	ϵ	∞		$\geq n$	$-\left(1-\frac{f}{n}\right)\log(n+f)+\frac{f}{n}\log f$
	Timed		ϵ	∞		≥ 1	total # of senders
Dynamic Pool	Cottrell[14]		ϵ	∞		≥ 1	total # of senders
	Threshold & Timed		ϵ	∞		$\geq n$	total # of senders

[표 1] Mix의 구성 형태에 따른 딜레이와 익명성 측정(n : threshold, t : 주기, : pool)

것 또는 Decision Diffie-Hellman problem을 푸는 것으로 환원(reduction)하는 것이다. 그 뒤로 긴 길이의 입력을 빠르게 처리하고, 최적의 강건함(Robustness)을 보이는 Hybrid Mix-Net이 고안되었고, Mix로 전달되는 메시지에 MAC(Message Authentication Code)을 사용함으로써 메시지 자체에 대한 인증을 할 수 있다는 장점이 존재하는 네트워크였다 [10]. 또한 Mix를 통과하는 메시지의 길이를 일정하게 유지하고, 선택 암호문 공격(Chosen Cipher Attack)에 안전한 Hybrid Mix-Net을 구성하기도 했다 [11]. 최근 들어 Mix-Nets에 대해 re-encryption이라는 새로운 암호학적 기술들을 이용한 응용 분야가 많이 소개되고 있다 [13].

4. 결론

지금까지 영상 데이터를 안전하게 전송하기 위한 Mix-Nets의 유형들과 안전성에 대해 알아보았다. 또한 익명성 측정 방법과 결과에 대해서도 알아보았다. 이 같은 Mix-Nets을 구성하기 위해 데이터의 익명성을 저해하는 대부분의 일반적인 공격자 모델들을 체계화하고, 전반적인 Mixes 해설에 관한 이론적 증명에 기초한 접근법을 대안으로 찾는 데 연구가 계속되어야 할 것이다. 향후 유비쿼터스 시대를 맞아 Ad-hoc 환경에서 영상 데이터 전송 시 발생할 수 있는 보안상의 문제를 해결하기 위해 Mix-net의 여러 형태를 적절히 이용할 수 있도록 기술적 법률적 연구 또한 필요할 것이다.

[참고문헌]

[1] D.L. Chaum, "The Dining Cryptographers Problem: Unconditional Sender and Recipient Untraceability", J. Cryptology, Vol. 1, No. 1, Springer-Verlag, 1988, pp. 65-75.

[2] Andreas Pfitzmann an Marit Kohntopp,"Anonymity, Unobservability, and Pseudonymity : A Proposal for Terminology", Draft, version 0.14, July 2000.

[3] D.J. Farber and K.C. Larson, "Network Security Via Dynamic Process Renaming", Fourth Data Communication Symp., Quebec City, Canada, Oct. 1975, pp. 8-18.

[4] P.A. Karger, "Non-Discretionary Access Control for decentralized Computing Systems", Master Thesis, MIT, Laboratory for Computer Science, Report MIT/LCS/TR-179, 1977.

[5] D.L. Chaum, "Untraceable Electronic Mail, Return Addresses, and Digital Pseudonyms", Comm. ACM, Feb. 1981, Vol. 24, No. 2, pp. 84-88.

[6] A. Ptzmann "Dienstintegrierende Kommunikationsnetze mit teilnehmeruber- prufbarem Datenschutz", IFB 234, Springer-Verlag, Heidelberg, 1990.

[7] C. Gulcu and G. Tsudik, "Mixing Email with Babel", Proc. Symposium on Network and Distributed System Security, San Diego, IEEE Comput. Soc. Press, 1996, pp. 2-16.

[8] L. Cottrell. "Mixmaster and remailer attacks", 1994. http://www.obscura.com/~loki/remailer/remailer-essay.html.

[9] Ohkubo, M., and Abe, M. "A length-invariant hybrid mix. In Advances in Cryptology ASIACRYPT 2000 (2000), T. Okamoto, Ed., vol. 1976 of LectureNotes in Computer Science, pp. 178-191.

[10]Jakobsson, M., and Juels, A. "An optimally robust hybrid mix network." In 20th Annual ACM Symposium on Principles of Distributed Computing (PODC 2001) (2001), ACM Press, pp. 284-292.

[11]Bodo Moller, "Provably Secure Public-Key Encryption for Length-Preserving Chaumian Mixes", CT-RSA 2003, Springer-Verlag LNCS 2612, pp. 244-262.

[12]Andrei Serjantov and Roger Dingledine and Paul Syverson, "From a Trickle to a Flood: Active Attacks on Several Mix Types", In the Proceedings of Privacy Enhancing Technologies workshop(PET 2002), April 2002.

[13]Philippe Golle, Markus Jakobsson, Ari Juels, and Paul Syverson, "Universal Re-Encryption for Mixnets", In the Proceedings of the 2004 RSA Conference, Cryptographer's track, San Francisco, USA, February 2004.

[14]L. Cottrell. "Mixmaster and remailer attacks", 1994.http://www.obscura.com/~loki/remailer/remailer-essay.html.