ML-IPSec Zone-mapping에 대한 연구

김정식 박진호 최경호 임을규

한양대학교 정보통신대학

nukuku@ihanyang.ac.kr pjh0347@yahoo.co.kr ckh820520@naver.com imeg@hanyang.ac.kr

Study of ML-IPSec Zone-mapping

Jung Sik Kim Jin Ho Park Kyoung Ho Choi Eul Gyu Im

College of Information Communications, Hanyang Univ.

요 약

IP의 보안문제를 해결하기 위해 IPSec architecture가 개발된 이후 여러 부분에서 IPSec을 사용할 수 있게 되었다. 하지만 IPSec은 전체 packet을 encryption을 해주기 때문에 intermediate node에서는 original IP protocol 형식의 packet에는 접근할 수 없게 되었다. 여기서 문제는 기존의 network의 성능을 향상시키기 위해 사용하는 기술들이 encryption되는 부분의 정보를 많이 사용한다는 점이다. 그래서 IPSec을 사용하게 되면 이 기술들을 사용할 수 없게 되는데 이 문제를 해결하기 위해 Multiple IP Security(ML-IPSec) protocol이 제안되었다. ML-IPSec을 사용하게 되면 이 intermediate node에서 encryption된 packet 중 필요한 부분만을 접근할 수 있게 되는데 이 ML-IPsec도 몇몇 문제점을 가지고 있게 되었다. 다시 이 문제를 해결하기 위한 방법이 제시되었는데 이 논문에서는 기존에 ML-IPSec 문제의 해결방안이 아닌 다른 시각에서의 해결법을 생각해 보았다.

1. 서 론(Introduction)

정보보호가 중요한 이슈로 떠오르면서 기존 IP protocol의 보안상 문제점을 해결해 [1]주기 위해 IP를 대체할 IPSec architecture가 개발되었다. 이 IPSec은 authentication, encryption 등을 이용하여 network layer에서 효율적인 end-to-end security를 보장해 주지만 기존 IP header와 그 상위의 모든 header, data를 encryption 해주기 때문에 end host를 제외한 네트워크의 intermediate node(router)들에서는 기존의 packet에 접근할 수 없었다. 하지만 기존의 network성능 향상을 위한 여러 기술들은 이 encryption되는 부분의 정보를 많이 사용하기 때문에 IPSec을 사용하게 되면 이 다양한 기술들을 사용하지 못하게 된다.

그래서 이 문제점을 해결하기 위해 ML-IPSec이 제안 되었는데 ML-IPSec은 intermediate node에서 IPSec의 일정 부분에 접근을 할 수 있게 해 주었다. 하지만 ML-IPSec도 몇몇 문제점을 가지게 되어서 Joel Sing과 Ben Soh가 이에 대한 문제점을 분석을 하였다.

이 논문의 2절에서는 IPSec의 동작방식과 어떤 부분이 encryption이 되는가, 왜 이 부분이 문제가 되는가, ML-IPSec이 무엇이고 어떻게 IPSec의 문제를 해결할 수 있는지를 알아보았다. 3절에서는 기존연구에서 발견한 ML-IPSec의 문제점을 요약하였고 4절에서 기존연구의 해결법을 요약해 두었다. 마지막으로 5절에서 새로운 해결법을 제시해 보게 된다.

1) 본 연구는 한국과학재단 특정기초연구(R01-2006-000-11196-0)지원으로 수행되었음.

2. Background

2.1 IPSec

IPSec이란 Internet Protocol Security의 약자로 network layer에서 사용하던 IP protocol의 보안 능력을 보안하기 위해 고안된 architecture로서 강력한 end-to-end security를 보장해 주게 된다.

IPSec은 두 traffic security protocol을 지원해 주게 되는데 AH(Authentication Header)와 ESP(Encapsulating Security Header)이다. 이 두 protocol은 각각 transport mode와 tunnel mode로 동작을 하게 되는데 transport mode는 IP보다 상위 계층을 보호하기 위한 동작 mode이고, tunnel mode는 IP datagram전체를 보호하는 동작 mode이다.

이 중 IPSec에서 문제가 되는 부분은 encryption을 사용하는 부분인데 AH mode를 사용할 때는 encryption을 하지 않지만 ESP mode를 사용하게 될 때 encryption을 수행하게 되므로 문제가 발생하게 된다. 그림 1에서와 같이 TCP packet에서 transport mode는 TCP header까지 encryption을 수행하고 tunnel mode는 original IP header까지 encryption을 해주게 된다.