스마트폰 보안을 위한 방화벽 모델

조유진, 최경, 도인실, 채기준
이화여자대학교 컴퓨터공학과
e-mail : eugene403@gmail.com, cbk0907@ewhain.net, isdoh@ewhain.net, kjchae@ewha.ac.kr

Firewall Model for Smartphone Security

Eugene Jo, Kyung Choi, Inshil Doh, Kijoon Chae
Dept. of Computer Science and Engineering, Ewha Womans University

요 약

스마트폰의 보급과 더불어 보안에 관한 관심도 크게 증가되고 다양한 보안 솔루션들이 제안되고 있다. 스마트폰 보안은 스마트폰의 이동성, 메모리 제약, 배터리의 한계, 동시에 실행되는 다른 프로세스들과의 충돌 고려 등의 요인으로 인해 접근하기가 어렵다. 또한 현존하는 스마트폰 방화벽 애플리케이션의 경우 많은 사용자가 불편함을 느끼고 사용을 해제하는 경우가 많다. 본 논문에서는 이와 같은 스마트폰의 특성과 제약사항을 고려해 방화벽을 살펴보고 스마트폰에 알맞은 방화벽 애플리케이션 모델을 제안하고자 한다.

1. 서론

최근 스마트폰에 대한 높은 관심과 함께 보급 역시 빠른 속도로 이루어지고 있다. 그러나 스마트폰의 빠른 보급 속도에 비해 스마트폰 보안은 아직 취약한 점이 많다. 특히 스마트폰 보안의 경우 데스크탑과 달리 한정된 배터리 파워와 메모리 등의 제약 사항으로 인해 기존 데스크탑 환경에서의 보안 기술을 그대로 적용하기에 어려움을 겪고 있다.

보급 속도에 미치지 못하는 스마트폰 보안의 부실로 발생한 많은 피해 사례 들 중 다수를 차지하고, 사용자들에게 큰 위협을 주는 것 중의 하나로 국제전화 발신으로 인한 과금과 개인 정보 유출이 있다. 여러 피해 사례 중에서도 사용자에게 금전적인 손실과 정보 유출로 불이익을 겪게 되는 이런 피해를 방지하기 위해 보안 기술 중 고전적이고 기본적인 방화벽을 사용한 애플리케이션들이 몇몇 마켓에 출시되었고 사용되고 있다.

데스크탑 환경에서의 방화벽이란 외부로 오고 가는 데이터를 허용하거나 거부하는 하드웨어 또는 소프트웨어로 데스크탑 보안에서도 기본적으로 설정된 요소이다. 고전적인 보안 기술의 하나로 많은 발전을 거쳐왔지만 아직 스마트폰 환경에서의 방화벽은 미진한 점이 많다.

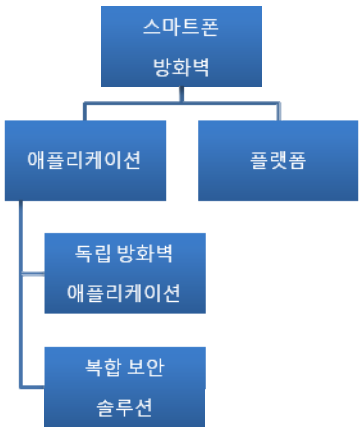
가벼움을 중시하는 스마트폰에서 구동되는 방화벽 애플리케이션의 경우, 네트워크 계층에서 IP 헤더를 보고 정해진 규칙에 의해 데이터 패킷의 허용 여부를 결정한다.

그러나 들어오는 패킷만을 확인하는 이런 방화벽 모델로는 외부로 전송되는 국제전화나 개인 정보 유출에 대한 방지를 할 수 없다. 본 논문에서는 데스크탑과는 다른 스마트폰의 특성을 고려하여 단방향성이 아닌 양방향성 방화벽 애플리케이션 모델을 제안하고자 한다.

2. 관련 연구

스마트폰 보급 이후 개발된 방화벽 솔루션들을 살펴보면 크게 어느 부분을 기준으로 개발되었느냐에 따라 그림 1 과 같이 애플리케이션 솔루션과 플랫폼 솔루션으로 구분할 수 있다.

애플리케이션 방화벽 제품들을 살펴보면 그 특성에 따라 다시 두 가지로 나뉘어지는데, 단독적으로 방화벽 기능만을 제공하는 애플리케이션과 통합적으로 제공하는 보안 솔루션 안에 방화벽 기능이 포함된 애플리케이션으로 나뉘어진다.



[그림 1] 스마트폰 방화벽 분류

위 구분을 바탕으로 현존하는 솔루션들을 좀 더 상세히 살펴보면 [표 1]과 같다.

[표 1]에서 알 수 있듯이 애플리케이션 방화벽은 배터리, 메모리의 제약으로 인해 단순한 차단 기능만을 갖고 있음을 볼 수 있다.

[표 1] 방화벽 제품 및 솔루션

특징	제품명	솔루션
독립 방화벽 애플리케이션	Smobile	Wireless hostspot에서 오는 직접적 공격이나 스캔에 대비한 파이어월
	DroidWall	IP Table을 이용해 유저가 작성한 White List 이외의 애플리케이션 트래픽은 전송받지 않음
복합 보안 솔루션	ESET Mobile Security 1.3	전체적인 모바일 보안 관리 시스템 속에서 방화벽 기능을 제공하며, 사용자가 작성한 리스트를 바탕으로 트래픽의 허용/차단을 관리
	F-Secure Mobile Security 6.1	
	Kaspersky Mobile Security 9	
	Trend Micro Mobile Security 6.5	
플랫폼	PaloAlto	방화벽 장비로 기존의 파이어월 기술에 스마트폰 애플리케이션과 관련된 인증 기술을 사용하는 파이어월 솔루션
	시큐아이	PaloAlto와 제휴한 국내 업체로 PaloAlto의 솔루션 제공

본 논문에서 제안할 스마트폰 애플리케이션 방화벽 모델과 관계가 깊은 방화벽 기능만을 제공하는 애플리케이션 방화벽 솔루션 제품에는 SMobile, DroidWall 이 있다.

앞서 언급한 두 제품의 방화벽 솔루션은 안드로이드 기반 스마트폰에서의 방화벽으로, 공통적으로 리눅스 커널의 IP Table 에 기반해 패킷 필터링만을 제공하고 있다. 들어오는 데이터 패킷의 헤드의 정보를 보고 정립된 규칙에 따라 차단하는 방식이지만 특정 애플리케이션 트래픽을 차단할 뿐, 웹 필터링까지 제공하지는 않는다.

Smobile 은 무선 핫스팟에서 오는 직접적 공격이나 스캔에 대비한 방화벽으로 네트워크 계층에서 패킷을 보고 차단한다. 그러나 웹 서핑시 웹에서 오는 트래픽은 감시하지 않기 때문에 이 부분에 있어 취약한 면모를 보이고 있다.

DroidWall 은 애플리케이션 트래픽 차단을 수행하며, 사용자가 White List 로 등록한 애플리케이션 이외의 트래픽은 전송받지 않는다. DroidWall 역시 IP Table 에 기반해 네트워크 계층 방화벽 기술을 사용하고 있다.

3. 제안 모델

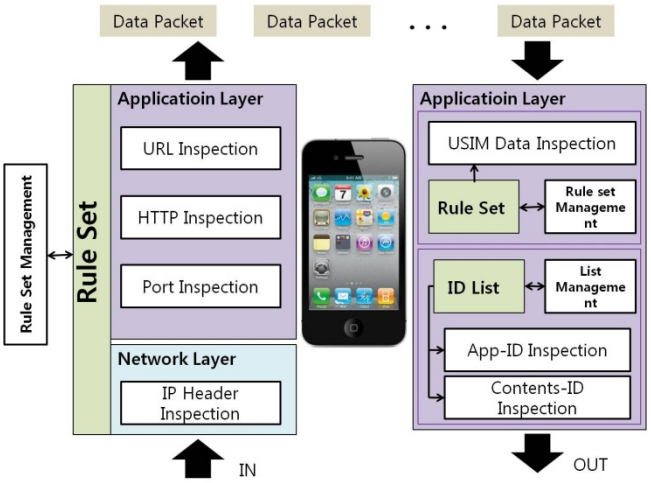
기존 스마트폰 방화벽 애플리케이션을 살펴보면, 단순한 패킷 필터링 기능만을 제공하고 있으며 스마트폰에서 많이 사용하는 웹 브라우저로 들어오는 웹 정보에 대한 필터링은 제공하지 않아 기능을 꺼두는 사용자가 많다.

또한 단순히 들어오는 패킷 헤더 정보만을 확인하고 있기 때문에 실질적으로 피해 사례의 다수를 차지하는 국제전화 발신과 개인 정보 유출에 있어서는 무력한 모습을 보이고 있다.

그렇기 때문에 본 논문에서는 incoming data packet 뿐만 아니라 outgoing data packet 까지 검증하는 방화벽 모델을 제시하고자 한다.

또한 현존하는 방화벽 애플리케이션은 네트워크 계층에서 IP 헤더만을 보고 허용 여부를 판단하기 때문에 원치 않는 프로토콜 트래픽 차단은 불가능하다. 스마트폰으로 웹 탐색 중 발생할 수 있는 보안 위협이나 스마트폰 간의 파일 전송시 발생할 수 있는 위협을 방지하기 위해 제안하고자 하는 모델은 응용 계층의 검증도 수행한다.

제안하고자 하는 모델을 간략히 도식화하면 하단의 [그림 2] 와 같다.



[그림 2] 제안하는 양방향 방화벽 모델

들어오는 데이터 패킷의 경우 위 모델에서는 네트워크 계층과 응용 계층, 두 가지 계층의 검사를 통과하게 된다. 공통적으로 적용되는 규칙 세트(Rule Set)가 있어 해당 규칙에 따라 검사를 수행하게 된다.

이 규칙 세트는 Rule Management 모듈에 의해 관리되며 Rule Management 는 사용자와 애플리케이션 서비스 주체에 의해 갱신되며 이 모듈에서 갱신된 규칙과 적용 여부가 규칙 세트에 반영되어 검사를 수행한다.

정해진 규칙 세트에 기반해 스마트폰으로 들어오는 데이터 패킷은 먼저 네트워크 계층에서 IP 헤더 검증을 거치고, 응용 계층으로 이동해 웹 트래픽인 경우 URL 과 HTTP, Port 검사를 거친 후 사용자가 데이터 패킷을 사용할 수 있다.

또한, Port 검사 모듈은 웹 트래픽 뿐만 아니라 스마트폰 간에 빈번하게 일어나는 파일 전송 시 발생하는 위협을 방지하기 위해 Rule Set Management 모듈에서 송신 허가 여부를 지정해 그 규칙에 기반해 검사가 수행된다.

이 모델에서는 들어오는 패킷만 검증하던 기존 방화벽 애플리케이션과 달리 나가는 패킷 역시 검증을 거치게 된다. 사용자 모르게 의도적으로 국제전화를 사용하도록 설정한 애플리케이션과 USIM 개인 정보 유출로 인한 피해 사례가 다수를 차지하고 있고, 사용자에게 큰 피해를 끼치고 있기 때문에 방화벽에서

나가는 패킷의 검증 역시 중요하기 때문이다.

외부로 나가는 패킷의 경우에 패킷의 IP 헤더 검사는 개인 정보 수집을 목적으로 할 경우 행선지가 수시로 바뀌기 때문에 갱신을 해 규칙 세트에 등록을 해 놓더라도 무의미하다. 따라서 나가는 패킷은 응용계층의 검사만을 수행한 후 3G, WiFi 망 등으로 빠져나가게 된다. 나가는 패킷 검증에서 중요한 부분은 나가는 데이터 패킷 속에 USIM 정보가 포함되어 있는지, 사용자가 쓰길 원치 않는 컨텐츠나 애플리케이션이 외부로 나가는지 검증하는 것이다. 이 검증을 위해서는 규칙 세트와 ID List 모듈이 필요하다. 규칙 세트 관리 모듈은 데이터 패킷 내에 USIM 정보가 포함될 경우 외부로의 전송을 허가하지 않도록 관리하며 이 관리 모듈에 의해 지정된 규칙 세트에 기반해 데이터 패킷의 내용을 검사한다. ID List 모듈은 밖으로 나가는 애플리케이션이나 컨텐츠의 ID 를 보고 외부와의 통신을 허가하지 않은 애플리케이션이나 컨텐츠가 외부로 나가려고 할 때 해당 패킷의 통과를 막아준다. 이 ID List 모듈 역시 허용하는 애플리케이션과 컨텐츠 ID 를 관리하기 위해 ID List Management 모듈이 필요하며 이 관리 모듈은 사용자와 방화벽 애플리케이션 서비스 제공자에 의해 관리된다.

4. 결론 및 향후 연구

다양한 스마트폰 제품이 출시되고 사용자들이 늘어나면서 스마트폰 보안에 대한 관심은 더욱 커져가고 있다. 본 논문에서는 스마트폰 특성에 따라 국제전화 과금, 개인 정보 유출 등의 피해를 막기 위한 방화벽 모델을 제안하였다.

스마트폰은 데스크탑 환경에서의 방화벽과 달리 한정된 배터리 수명과 메모리, 처리 환경 등의 많은 제약 사항이 있다. 이런 제약 사항을 고려했을 때, 스마트폰을 위한 가벼운 보안 해결책으로 방화벽을 제안했으며, 기존 데스크탑 환경과 달리 나가는 데이터 트래픽의 검증이 중요한 스마트폰 환경의 특성을 반영해 양방향 트래픽 검증을 수행하는 방화벽 모델을 제안하였다.

향후에는 제시한 방화벽 모델을 시뮬레이션을 통해 효율성을 분석해 보고 이를 바탕으로 실제적인 애플리케이션으로 구현하고자 한다..

5. 참고문헌

[1] Smobile. http://www.smobilesystems.com/

[2] DroidWall. http://code.google.com/p/droidwall/

[3] Palo Alto Networks. http://www.paloaltonetworks.com/

[4] 시큐아이. http://www.secui.com/

[5] AV comparatives, “Product Review; Mobile Security,” 2010. http:// www.av-comparatives.org.

[6] Chuanxiong Guo, Helen J. Wang, Wenwu Zhu, “Smart-Phone Attacks and Defenses,” In HotNets III, 2004.

[7] Hao Yu, Ming-Xiang He, Hai-chun Sun, “The Design of Firewall in Mobile Phone Based on Cross-Layer Collaboration,” Asian Network for Scientific Information, 2009.

[8] Asaf Shabtai, “Malware Detection on Mobile Devices,” 2010 Eleventh International Conference On Mobile Data Management, 2010.

[9] Asaf Shabtai, Yuval Fledel, Yuval Elovici, Shlomi Dolev, Chanan Glezer, “Google Android:A Comprehensive Security Assessment,” IEEE Security&Privacy, 2010.