DOI: 10.3745/KIPSTC.2009.16C.6.691

휴대용통신단말의 효과적인 보안관리를 위한 보안 재구성기법의 설계 및 구현

안 개 일[†] · 김 기 영[††] · 서 동 일[†††]

요 약

휴대용 통신 단말은 스마트 폰이나 PDA와 같은 통신 서비스를 제공하는 작은 크기의 휴대용 컴퓨터이다. 현재 휴대용 통신 단말의 발전을 가로막는 가장 큰 장벽중의 하나가 바로 보안이다. 비록 휴대용 통신 단말을 보호할 수 있는 다양한 보안기술들은 있지만, 휴대용 통신 단말은 데스크톱 컴퓨터에 비해 컴퓨팅 자원이 빈약하고 사용자 인터페이스가 불편하여 그 보안기술 모두를 휴대용 통신 단말에 운용할 수 없기 때문이다. 본 논문에서는 휴대용 통신 단말의 보안을 효과적으로 관리할 수 있는 상황인지형 보안재구성 기법을 제안하고 설계한다. 본 보안재구성 기법은 휴대용 통신 단말의 현재 보안 상황에 가장 적합한 최적의 보안 서비스를 자동으로 제공할 수 있다. 본 제안하는 기법의 구현과 실험을 통하여 본 기법이 보안수준을 떨어뜨리는 것 없이 자원 효율성과 사용자 편의성에서 우수하다는 것을 확인하였다.

키워드 : 단말기보안, 보안관리, 휴대용통신단말, 보안상황, 보안재구성

Design and Implementation of Security Reconfiguration for Effective Security Management of Mobile Communication Device

Gaeil An[†] · Kiyoung Kim[††] · Dongil Seo[†††]

ABSTRACT

A mobile communication device is a small size of portable computer which provides communication service, such as smart phone and PDA. Currently, one of the biggest barriers in developing the mobile communication device is security issue. Even though there are excellent security functions which can remove the security issues, there is a problem that the mobile communication device can not be loaded with all the functions because it has low storage, poor computational power, and inconvenient user interface, compared to the desktop personal computer. This paper proposes a context-aware security reconfiguration scheme for effective security management of the mobile communication device. The scheme can provide the mobile communication device with the optimized security service which is most adapted to its current security context. Through the prototype implementation and the experiments of the proposed scheme, we have confirmed that the proposed scheme is excellent in terms of computing resource efficiency and usability, without degrading security level.

Keywords : Device Security, Security Management, Mobile Communication Device, Security Context, Security Reconfiguration

1. 서 론

휴대용 통신 단말은 휴대폰이나 PDA (Personal Digital Assistant)와 같이 통신 서비스를 제공하는 작은 크기의 휴대용 컴퓨터이다. 초기의 휴대용 통신 단말은 전화와 같은 하나의 통신 서비스만을 제공하였지만, 현재는 CDMA, WiFI와 같은 이종의 통신 장치를 지원하는 멀티 통신 서비스와, 카메라, 네비게이션 등과 같은 다양한 멀티미디어 서비스를 모두 하나의 단말에서 통합하여 제공할 수 있도록 진화하고 있다[1].

휴대용 통신 단말이 전화 서비스만을 제공하는 시절에는 암호와 같은 사용자 인증 정도만을 제공하더라도 보안측면에서 크게 문제될 것이 없었다. 그러나 휴대용 통신 단말의 발전으로 사용자의 중요 개인정보가 휴대용 통신 단말에 저장되고 휴대용 통신 단말이 다양한 통신 네트워크에 노출됨에 따라 보안의 중요성이 점점 더 크게 강조되고 있다.

휴대용 통신 단말은 데스크톱 개인용 컴퓨터 및 무선 시스템에 해당되기 때문에 기존의 보안 문제가 휴대용 통신 단말에도 그대로 내재되어 있으며, 또한 통신 및 멀티미디어 서비스를 통합된 형태로 제공하기 때문에 새로운 형태의

※ 본 연구는 지식경제부 및 한국산업기술평가관리원의 IT R&D program의 일환으로 수행하였음. [2008-S-006-01, "복합단말용 침해방지 기술개발"]
† 정 회 원 : 한국전자통신연구원 인프라보호연구팀 선임연구원
†† 정 회 원 : 한국전자통신연구원 인프라보호연구팀 책임연구원
††† 정 회 원 : 한국전자통신연구원 인프라보호연구팀 팀장
논문접수 : 2009년 8월 31일
수 정 일 : 1차 2009년 10월 6일
심사완료 : 2009년 10월 12일

공격에도 취약할 수 있다[2]. 이러한 모바일 보안 위협을 방어하기 위해서는 개인 방화벽이나 개인정보 유출방지 프로그램 등 다양한 종류의 보안 기능들이 휴대용 통신 단말에 운용되어야 한다. 그러나 휴대용 통신 단말은 데스크톱 컴퓨터와 비교할 때 컴퓨팅 자원이 매우 빈약하기 때문에 모든 요구되는 보안 기능을 탑재하기 어려우며, 또한 사용자 인터페이스가 매우 불편하기 때문에 보안 기능을 설정하고 운용하는 작업이 쉽지 않은 문제가 있다.

본 논문에서는 휴대용 통신 단말을 위한 상황인지형 보안재구성 기법을 제안한다. 본 기법은 휴대용 통신 단말의 보안 상황을 감지하여 현재의 상황에서 가장 최적화된 보안 서비스를 자동으로 구성함으로써 보안수준을 떨어뜨리는 것 없이 자원 효율성과 사용자 편의성을 극대화 시키는 것을 목적으로 한다.

본 논문의 차례는 다음과 같다. 2장에서는 휴대용 통신 단말의 특징과 보안 위협을 살펴보고, 3장에서는 상황인지형 보안재구성 기법을 제안한다. 4장에서는 프로토타입 시스템 구현을 통하여 그 성능을 분석하고, 5장에서 결론을 맺는다.

2. 휴대용 통신 단말의 특징 및 보안 위협

휴대용 통신 단말은 휴대폰이나 PDA와 같이 통신 서비스를 제공하는 작은 크기의 휴대용 컴퓨터이다. 초기의 휴대용 통신 단말은 휴대용 전화기와 같이 단순히 하나의 통신 서비스를 제공하는 수준이었다. 그러나 현재는 CDMA, Bluetooth, WiFi, Wibro 등과 같은 이종의 통신장치를 지원하는 멀티 통신 서비스와 IPTV, DMB(Digital Multimedia Boradcasting) 등과 같은 다양한 멀티미디어 서비스를 모두 통합하여 하나의 단말에서 제공할 수 있도록 진화하고 있다.

휴대용 통신 단말은 데스크톱 컴퓨터와 비교할 때 다음과 같은 특징을 갖는다.

- 불편한 사용자 인터페이스: 스크린이 작고 키보드를 통한 입력이 불편함
- 배터리 사용
- 빈약한 컴퓨팅 자원: CPU, 메모리 등 컴퓨팅 성능이 제한적임
- 멀티 통신 장치: USB, Bluetooth, WiFi, CDMA 등 다양한 통신 장치를 제공함
- 통합 단말: 네비게이션, DMB, 카메라, MP3 플레이어 등의 서비스를 하나의 단말에서 제공함

초기의 휴대용 통신 단말은 사용자 인증 정도만으로도 그 보안 요구사항을 충족시킬 수 있었지만, 사용자들의 중요 개인정보가 휴대용 통신 단말에 저장되고 휴대용 통신 단말이 다양한 통신 네트워크에 노출되면서 휴대용 통신 단말에 대한 보안 위협이 크게 증가되고 있다. 휴대용 통신 단말은 소형 컴퓨터인 동시에 이동형 무선 시스템에 해당되기 때문에 바이러스, 트로이 목마, 웜과 같은 전통적인 컴퓨터 보안 공격뿐만 아니라 무선 도청(eavesdropping)이나 전파 방해(jamming) 등과 같은 전형적인 무선 보안 공격에도 원천적으로 취약한 특성을 갖는다. 더욱이 휴대용 통신 단말은 이동성 특징으로 인하여 크로스 서비스 공격[3]과 배터리 소모 공격[4][5][6], 그리고 도난 및 분실과 같은 새로운 위협에도 노출되어 있다.

새로운 유형의 공격에 대하여 좀 더 자세히 살펴보도록 한다. 먼저, 크로스 서비스 공격은 다양한 통신 장치가 하나의 휴대용 통신 단말에 통합되어 서로 다른 통신 서비스의 경계를 자유롭게 넘어가는 것을 허용하기 때문에 발생하는 공격이다. 크로스 서비스 공격은 공격 목표인 통신 서비스를 직접 공격하는 것이 아니라, 보안이 취약한 통신 서비스를 먼저 공격하여 단말을 감염시킨 후 본래 목표인 통신 서비스를 무단으로 사용하는 공격이다. 예를 들어, CDMA, WiBro, WiFi 통신 서비스를 제공하는 휴대용 통신 단말을 공격하여 CDMA와 WiBro 서비스를 무단으로 사용하고자 할 때, 크로스 서비스 공격은 보안 취약점이 거의 없는 CDMA 폰 서비스를 공격하는 것이 아니라, 상대적으로 보안이 매우 취약한 WiFi 인터페이스를 먼저 공격하여 그 모바일 단말을 감염시킨 후, 최종적으로 WiBro 및 CDMA 폰 서비스를 마음대로 제어하는 공격방식을 사용한다. 공격자는 감염된 단말의 통신 인터페이스를 통하여 다른 단말에 스팸, 피싱, 복제 등의 공격을 실행할 수 있으며, 또한 유료인 CDMA 폰 서비스를 무단으로 사용함으로써 과금 공격을 실행할 수도 있다.

크로스 서비스 공격을 방어하기 위한 기법으로써 레이블(label)기반의 접근제어방식[3]이 제안되었다. 이 방식은 프로세스가 컴퓨팅 자원(레이블로 식별됨)을 접근하는 것을 모니터링하면서, 프로세스별 접근된 컴퓨팅 자원에 대한 접근상태정보를 생성하고, 그 접근상태정보와 사전에 설정된 접근제어정책을 기반으로 하여 프로세스가 컴퓨팅 자원을 접근하는 것을 허용 또는 거부할지 결정하는 방식이다.

배터리 소모 공격은 서비스 거부 공격의 일종으로써 단말이 절전(sleep) 모드로 들어가는 것을 막음으로써 단말의 배터리를 빠르게 방전시키는 공격이다. 배터리 소모 공격은 악성, 양성, 그리고 서비스 요구공격으로 분류될 수 있다[4]. 악성 공격은 컴퓨팅 자원을 크게 소모시키는 바이러스 공격으로써 Cabir 바이러스가 하나의 예이다. Cabir 는 Symbian OS 기반의 폰에서 동작하는데 다른 폰을 감염시킬 뿐만 아니라 Bluetooth 전파를 계속 브로드케스트함으로써 감염된 폰의 배터리도 방전시킬 수 있는 바이러스이다. 양성 공격은 악성 코드는 포함하고 있지 않지만, 단말에서 실행되면 배터리가 많이 소모될 수 있도록 컴퓨팅 자원을 과도하게 사용하는 컴퓨터 데이터 (예, 용량이 큰 사진 파일) 및 응용 프로그램을 유포하는 공격이다. 마지막으로 서비스요구 공격은 모바일 통신단말이 제공하는 통신 서비스를 계속 반복해서 요구하는 공격이다.

배터리 소모 공격중에서 서비스 요구 공격을 약화시키기 위해 제안된 기법으로는 멀티계층 인증기법[5]이 있으며, 악

성 및 약성 공격을 탐지하기 위해 제안된 기법으로는 에너지 시그니처 모니터 기법[5]이 있다. 멀티계층 인증기법은 에너지 소모가 가장 작은 낮은 인증단계부터 에너지 소모가 가장 큰 높은 인증단계까지 여러 개의 계층을 두어서, 공격자가 낮은 인증단계를 통과하지 못하면 그 다음 단계를 갈 수 없도록 하여 서비스 요구 공격을 약화시키는 방법이다. 에너지 시그니처 모니터 기법은 응용 프로그램의 정상적인 에너지 소모를 시그니처화한 후 그 정상 시스니처와 다르게 배터리를 소모하는 프로그램을 공격으로 간주하는 방법이다. 에너지 시그니처 모니터 기법과 비슷한 기법으로써, 주어진 시간 동안 소비된 배터리를 측정하고 비정상적으로 많은 배터리를 소모하는 프로세스를 공격으로 탐지하는 방법[6]도 있다.

마지막으로, 휴대용 통신 단말은 휴대용 컴퓨터이기 때문에 도난 및 분실에 매우 취약하며, 따라서 개인 정보가 외부로 유출될 수 있는 위협에 노출되어 있다. 개인 정보가 외부로 유출되는 것을 방지하기 위한 방법으로써 중요 데이터 암호화와 원격 삭제 방법이 제안되고 있다.

3. 상황인식기반의 보안재구성 기법

3.1 보안관리 요구사항

휴대용 통신 단말은 기존의 공격뿐만 아니라 새로운 유형의 공격에도 취약하기 때문에 인증, 암호, 바이러스 스캔너, 방화벽, 네트워크 침입탐지와 같은 전통적인 보안기능뿐만 아니라 크로스 서비스 공격 방어를 위한 컴퓨팅자원 접근제어, 비정상 배터리 소모 탐지, 중요데이터 유출방지 등과 같은 보안기능도 탑재될 필요가 있다.

그러나 이러한 보안 기능을 휴대용 통신 단말에 운용할 때 다음과 같은 두 가지 문제가 있을 수 있다. 성능 저하와 사용 불편이 바로 그것이다. 성능 저하는 사용 불편보다 더 심각한 문제일 수 있다. 이전 절에서 언급했듯이, 휴대용 통신 단말의 가장 큰 제약 사항중의 하나가 빈약한 컴퓨팅자원이다. 보안 기능은 일반적으로 프로세스, 파일, 네트워크 패킷 등의 모니터링 및 필터링 오퍼레이션을 필요로 하는데, 이것은 CPU, 메모리 등의 시스템 자원을 많이 소모하는 작업이기 때문에 자원이 빈약한 휴대용 통신 단말입장에서는 큰 부담이 아닐 수 없다. 즉, 보안기능을 휴대용 통신 단말에 운용하는 경우에 만약 사용자가 응답 지연 등 서비스 품질의 저하를 느낀다면 보안기능이 아무리 필수기능이라고 하더라고 그 효용가치는 크게 떨어질 것이다.

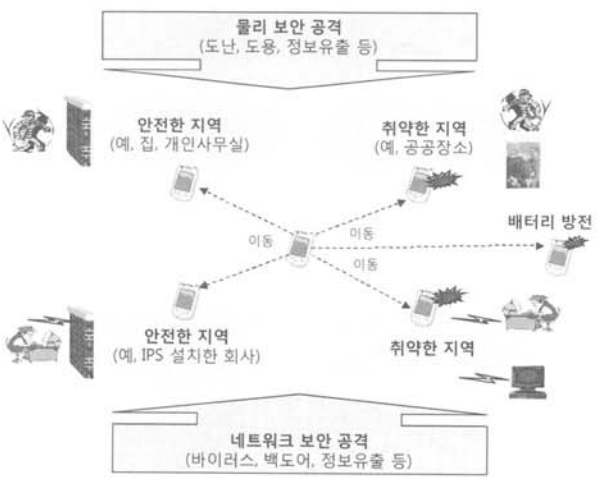
두 번째 문제는 사용불편이다. 보안기능을 운용할 때 보안 정책 구성 등 전반적인 관리가 필요한데, 휴대용 통신 단말은 사용자 인터페이스가 비교적 불편하기 때문에 사용자에게 보안 관리는 매우 귀찮고 어려운 작업이다. 예를 들어, 암호기반의 사용자 인증기능이 휴대용 통신 단말에 적용될 때 키보드 불편으로 인하여 암호를 입력하는 것이 사용자에게 고역일 수 있다.

휴대용 통신 단말에 적용될 수 있는 보안관리 서비스로써 다음과 같은 두 종류의 서비스를 가정할 수 있다.

(1) 최상의 보안관리 서비스 - 보안 취약성이 최악인 경우를 가정하여 최상의 보안 서비스 제공
(2) 최적의 보안관리 서비스 - 현재의 보안 취약성을 해결할 수 있을 정도의 보안 서비스 제공

최상의 보안관리 서비스는 가능한 모든 보안 기능을 휴대용 통신 단말에 실행시킴으로써 최고 수준의 보안 상태를 계속 유지할 수 있는 장점이 있지만, 필요 없는 보안 기능이 실행됨으로써 사용자에게 불편을 주고 컴퓨팅 자원도 낭비되는 단점이 있다. 이에 반하여, 최적의 보안관리 서비스는 휴대용 통신 단말의 현재의 보안 취약성을 해결할 수 있는 보안 기능만을 실행하기 때문에 사용자 편의성 및 자원 효율성을 높일 수 있는 장점이 있지만, 휴대용 통신 단말은 (그림 1)에 도시된 바와 같이 집, 공공장소, 회사 등 다양한 장소로 이동하는 이동성 특징을 갖기 때문에 휴대용 통신 단말이 다른 장소로 이동할 때마다 그 장소의 보안 취약점을 감지하여 그 장소에 맞는 최적의 보안서비스를 다시 구성해야 한다.

본 논문에서 제안하는 보안재구성기법은 휴대용 통신 단말에게 최적의 보안관리 서비스를 항상 제공할 수 있도록 휴대용 통신 단말이 다른 장소로 이동할 때 그 장소의 보안 취약점을 감지하여 그 장소에 맞는 최적의 보안서비스를 다시 구성하는 것이다. 휴대용 통신 단말의 보안 취약성은 각 단말이 현재 위치한 장소와 현재 접속한 네트워크에 따라서 그 정도가 다를 수 있다. 예를 들어, (그림 1)에서 휴대용 통신 단말이 집과 같은 개인용 공간으로 이동하는 경우에 그 단말은 도용 및 도난 등과 같은 물리적인 공격으로부터는 안전할 것이지만, 사람들이 많이 모여있는 공공장소로 이동하는 경우에는 물리적인 공격에 매우 취약할 것이다. 또한 휴대용 통신 단말이 무선 네트워크를 보호하기 위해 IPS와 같은 보안시스템을 설치한 지역으로 이동하는 경우에



(그림 1) 휴대용 통신 단말의 이동성과 보안취약성
(Fig. 1) Mobility and security vulnerability of mobile communication device

는 네트워크 보안 공격으로부터 안전하겠지만, 무선 네트워크 접속만 제공하는 지역으로 이동하는 경우에는 네트워크 보안에 매우 취약할 것이다.

보안재구성기법은 휴대용 통신 단말이 물리적 공격으로부터 안전한 지역으로 이동하면, 물리적 공격 방어에 효과가 있는 인증, 중요정보 유출방지기능과 같은 보안기능을 해제하거나 최소로 동작하도록 하고, 만약 네트워크 보안 공격으로부터 안전한 지역으로 이동하면 네트워크 보안 공격에 효과가 있는 방화벽, 바이러스 체크 등과 같은 보안기능을 해제 또는 최소로 동작하도록 함으로써 최적의 보안관리 서비스를 제공한다. 반대로 휴대용 통신 단말이 물리적 공격에 취약한 지역이나 또는 네트워크보안공격에 취약한 장소로 이동하면, 그 취약한 공격을 방어할 수 있는 보안기능을 실행하거나 또는 강화시킴으로써 최적의 보안관리 서비스를 제공한다. 효과적인 보안재구성을 제공하기 위해서는 휴대용 통신 단말이 이동한 장소의 보안 취약점, 즉 보안상황을 정확하고 빠르게 판단할 수 있는 메커니즘개발이 매우 중요하다.

3.2 보안상황 정보

본 논문에서 제안하는 휴대용 통신 단말의 보안재구성 기법은 현재의 보안상황을 감지하여 보안수준이 떨어지지 않도록 새로운 보안환경의 변화에 반응하는 것이다. 상황(context)이란 사람, 장소, 객체 등이 처한 현재의 상태나 입장을 특징 지우기 위하여 사용되는 정보를 말한다[7]. [8]과 [9]에서는 상황 정보를 다음과 같은 네 개의 범주로 구분하였다.

- 컴퓨팅 상황 (Computing context): 네트워크 연결 상태, 통신 대역폭, 그리고 프린터, 디스플레이, 워크스테이션과 같은 주변의 컴퓨팅 자원들
- 사용자 상황 (User context): 사용자의 프로파일, 위치, 주변의 사람들 등
- 물리적 상황 (Physical context): 조명, 소음 레벨, 교통상태, 온도 등
- 시간 상황 (Time context): 계절, 달, 주, 시간 등 [10]

본 논문에서는 보안 상황정보가 현재의 휴대용 통신 단말의 보안 상태를 파악하기 위한 중요한 본질적인 상황이라고 판단되어 다섯 번째 범주로써 보안 상황(Security context)을 제안한다. 보안 상황이란 휴대용 통신 단말의 용도(예, 게임용, 비즈니스용 등), 위치한 장소 (예, 회사, 집, 음식점), 접속한 네트워크에 설치된 보안기능(예, IDS, Firewall 등), 휴대용 통신 단말의 배터리 상태 등의 정보를 말한다. 단말의 현재 배터리상태 정보는 현재의 보안 상황에 반응할 때 현재 컴퓨팅 자원의 가용상태를 반영하기 위하여 보안 상황정보에 포함하였다.

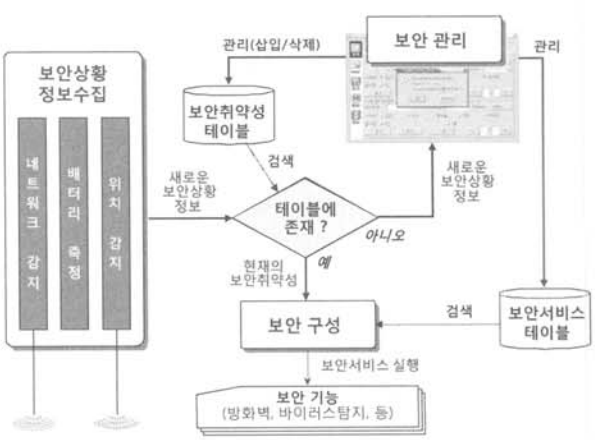
보안 상황정보는 휴대용 통신 단말의 현재 보안 취약성을 평가하는 데 사용된다. 예를 들어, "단말의 용도가 비즈니스용이고, 현재 음식점에 위치하고 있으며, 접속한 네트워크에 보안 기능이 설치되어 있지 않다"라는 보안상황 정보가 주어졌다면, 현재 휴대용 통신 단말은 바이러스, 웜 등의 네트워크 공격뿐만 아니라 도난, 도용 등의 물리적 공격의 위협에도 노출되어 있다고 평가할 수 있을 것이다.

휴대용 통신 단말의 현재 보안 취약성을 정확하게 평가하기 위한 가장 중요한 작업은 정확한 보안상황정보를 수집하는 일이다. 비록 본 논문에서 정의한 모든 보안상황정보를 자동으로 수집하는 것은 현재로써는 어렵지만, 향후 유비쿼터스 서비스가 실현되면 사용자가 현재 회사에 있는지 음식점에 있는지를 센서를 통하여 자동으로 인식할 수 있을 것이다. 모든 보안상황정보를 수집하는 것이 어려운 상황에서는 사용자가 보안상황정보를 직접 제공하거나 또는 보안 취약성 평가에 일부분 참여하게 함으로써 보안 취약성에 대한 평가의 정확도를 높일 수 있다.

3.3 구조 및 알고리즘

본 논문에서 제안하는 휴대용 통신 단말을 위한 상황인지형 보안 재구성의 구조는 (그림 2)에 도시된 바와 같이 보안상황정보수집 모듈, 관리 모듈, 보안구성 모듈 등 세 개의 모듈과, 보안취약성 테이블과 보안서비스 테이블 등 두 개의 테이블로 구성된다.

보안상황정보수집 모듈은 휴대용 통신 단말이 현재 접속한 네트워크 정보와 현재 위치한 장소, 그리고 배터리 상태 정보를 수집하는 모듈이다. 보안관리 모듈은 보안취약성 테이블과 보안서비스 테이블을 관리하는 모듈이다. 보안취약성 테이블은 <보안상황>과 <보안취약점> 필드로 구성된다. 각 <보안상황>필드는 현재 접속한 네트워크와 위치한 장소 정보에 의해 구별된다. <보안취약점>필드는 네트워크 공격, 바이러스, 중요정보유출, 도청, AP위장, 도난, 도용 등 네트워크 및 물리적 공격에 대한 위험 여부를 나타낸다. 보안서비스 테이블은 <보안기능>, <보안효과>, <운용스크립트>들로 구성된다. <보안기능>은 방화벽, IDS 등 보안기능 식별자를 말하며, <보안효과>는 각 <보안기능>이 방어할 수 있는 보안공격을 나타내며, 그 보안공격의 종류는 보안취약



(그림 2) 상황인식기반의 보안재구성의 구조
(Fig. 2) Architecture of context-aware security reconfiguration

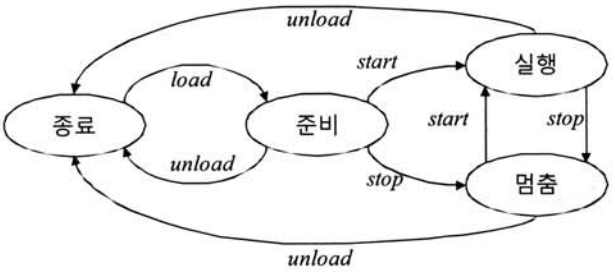
성 테이블의 <보안취약점>에서 정의된 공격명을 그대로 사용한다. 보안구성 모듈은 보안서비스 테이블을 참조하여 현재의 보안상황에 맞는 보안 서비스를 실행하는 역할을 한다.

본 논문에서 제안하는 상황인지형 보안 재구성 기법의 기본적인 동작 알고리즘은 다음과 같다. 먼저, 보안상황정보수집 모듈은 휴대용 통신 단말이 접속한 무선 네트워크, 위치한 장소, 그리고 배터리 상태 등 상황정보를 주기적으로 수집한다. 만약 보안상황이 바뀌었으면(예, 다른 무선 네트워크에 접속, 다른 장소로 이동, 또는단말 배터링 상태가 Low), 수집한 상황정보가 보안취약성 테이블(즉, <보안상황> 필드)에 저장되어 있는지 검색한다. 만약 그 수집한 정보가 보안취약성 테이블에서 없으면, 그 정보는 새로운 상황정보이므로 관리 모듈을 통해 사용자에게 제공하고, 그 보안상황에 대한 보안 취약성 평가를 받은 후 보안 취약성 테이블에 그 결과를 저장한다. 만약 그 수집한 상황정보가 보안취약성 테이블에서 발견되면, 그 상황정보에 해당하는 <보안취약점>정보를 검색한다. 마지막으로 보안서비스 테이블에서 그 <보안취약점>을 제거할 수 있는 <보안기능>을 검색(즉, <보안효과> 필드 사용하여 검색)하여 해당 <운용스크립트>를 실행한다.

본 보안 재구성 기법을 좀 더 쉽게 이해할 수 있도록, 간단한 예를 통해 설명하면 다음과 같다. 먼저, 휴대용 통신 단말은 두 개의 보안기능, 즉 도용을 방지할 수 있는 사용자 인증 보안기능과 네트워크 공격을 탐지할 수 있는 방화벽 보안기능을 탑재하고 있다고 가정하자. 이때 보안서비스 테이블은 [<보안기능>="사용자 인증", <보안효과>="도용공격">, <운용스크립트>=....] 로 구성된다. 보안상황정보수집 모듈은 단말이 현재 사용자의 "근무 회사"로 이동한 것을 감지하면, 그 상황정보가 보안취약성 테이블에(즉, <보안상황>필드에서 "근무 회사"가) 있는지 검색하고, 만약 없으면 사용자에게 보안 취약성 정보를 추천하면서 최종 평가를 받는다. 사용자가 "근무회사가 도용공격에 취약하다"라는 평가를 했다고 가정하자. 이제 그 보안상황정보와 보안취약성 정보는 보안취약성 테이블(즉, <보안상황>="근무 회사", <보안취약점>="도용공격")에 저장된다. 마지막으로 보안구성 모듈은 휴대용 통신 단말이 현재 도용 공격에 취약하므로 보안 서비스 테이블에서 도용공격을 방어할 수 있는 보안기능을 검색하며, 결국 사용자 인증기능이 검색되어 실행된다. 향후 휴대용 통신 단말이 회사로 이동했을 때에는, 회사에 대한 보안취약성 정보가 보안취약성 테이블에 저장되어 있기 때문에 사용자가 다시 등록할 필요가 없다.

본 보안재구성 기법이 관리하는 보안 기능의 생명주기는 (그림 3)에 도시되어 있다. 보안기능은 네 가지 상태, 즉 준비, 실행, 멈춤, 종료 상태로 변경될 수 있다. 본 논문에서는 보안기능의 상태를 변경할 수 있는 네 종류의 보안기능 운용 스크립트를 다음과 같이 정의하며, 이것의 목적은 보안기능을 자동적으로 관리하기 위함이다.

① Load : 보안 기능을 준비상태로 만들기 위해서 보안기능을 동작하는데 필요한 사전작업을 실행하는 스크립트



(그림 3) 보안기능의 생명주기
(Fig. 3) Life cycle of security function

② Unload: 보안 기능을 종료상태로 만들기 위해, 관련된 작업을 실행하고 보안기능을 종료시키는 스크립트
③ start: 보안 기능을 동작상태로 만드는 스크립트
④ stop: 보안 기능을 멈춤상태로 만드는 스크립트

본 보안 재구성 기법의 보안구성 모듈은 휴대용 통신 단말의 보안 상태가 "안전 상태"에서 "위험 상태"로 변경되면 그 보안취약점을 해결할 수 있는 해당 보안 기능을 준비시키기 위해 load 스크립트를 실행한다. 그 보안 기능은 "준비"상태가 된다. 곧이어 "준비"상태의 보안기능을 실제로 동작시키기 위하여 start 스크립트가 실행한다. 휴대용 통신 단말이 "위험상태"에서 "안전상태"로 바뀌면, "실행"상태인 보안기능을 중지시키기 위해서 stop 스크립트가 실행하며, 그때의 보안 기능은 "멈춤"상태가 된다. 또한 그 보안 기능을 완전히 종료시킬 필요가 있다면 unload 스크립트가 실행한다.

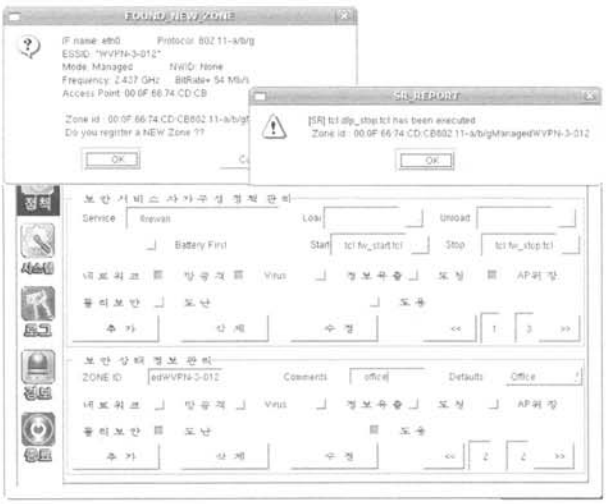
보안서비스 테이블에는 앞에서 언급한 바와 같이 네 종류의 스크립트를 저장하기 위한 <운용스클립트> 필드(즉, <load-운용스크립트>, <unload-운용스크립트>, ...)를 정의하고 있다.

4. 구현 및 성능평가

4.1 프로토타입 구현

본 논문에서는 제안한 보안재구성 프로토타입 시스템을 우분투(Ubuntu) 리눅스 플랫폼상에서 개발하였다. 보안기능 운용스크립트는 Tcl 언어를 사용하여 작성하였다. 본 프로토타입 시스템은 접속한 네트워크 정보와 배터리 상태정보를 수집할 수 있으며, 위치한 장소 정보는 현재 접속한 네트워크 정보를 기반으로 하여 사용자에 의해 수동으로 등록된다. 본 프로토타입 시스템은 보안 기능으로써 리눅스에서 자체적으로 제공하는 방화벽(firestarter)과 스크린세이버(xscreensaver), 그리고 본 연구팀에서 독자적으로 개발한 접근제어와 데이터유출방지 프로그램을 관리한다.

(그림 4)는 본 프로토타입 시스템의 GUI 화면이다. 그 GUI 화면에서, 보안 서비스, "firewall"은 네트워크공격과 바이러스를 방어할 수 있는 보안 기능이며, 그 보안 기능의 운용 스크립트로써 start와 stop 스크립트가 등록되어 있다.



(그림 4) 제안하는 기법의 프로토타입 시스템 GUI
(Fig. 4) Prototype system GUI of the proposed scheme

또한 ZONE ID가 "edWVPN-3-012"인 상황에서는 도난 및 도용 공격에 취약하다는 보안상황에 대한 보안취약성 정보도 등록되어 있다. 여기서, ZONE ID는 보안 상황에 대한 식별자로써, 접속한 네트워크 정보(예, SSID, AP의 IP 정보 등)를 사용하여 만들어졌다.

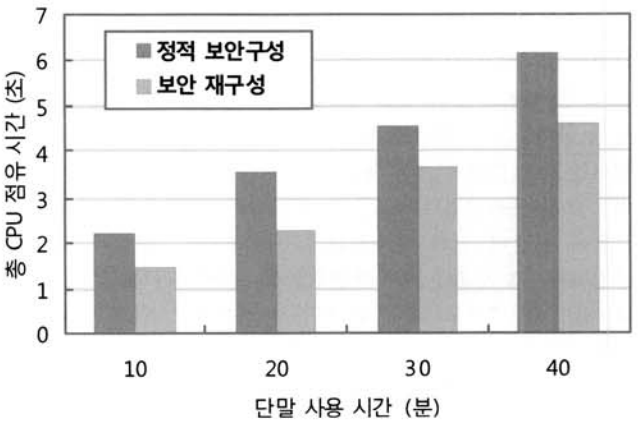
4.2 성능 평가

본 논문에서는 사용자 편의성관점에서 그 성능을 평가하기 위하여, 본 보안 재구성 프로토타입을 Wibrain의 B1 UMPC(Ultra-Mobile Personal Computer) 모바일 단말에 설치하고 (그림 1)과 같은 네트워크 환경(세 개의 AP를 사용하여 집, 회사, 공공장소로 가정함)에서 실험하였다. 비록 사용자가 새로운 보안상황을 접할 때에는 그 보안상황에 해당하는 보안 취약성을 직접 평가해야 하는 불편함은 있었지만, 그 보안상황이 등록된 후부터는 그 보안상황과 관련된 보안 서비스가 자동으로 구성되기 때문에 사용자 편의성에서 문제가 없음을 확인하였다. 즉, 모바일 통신 단말이 집에서 회사로 이동했을 때, 회사라는 장소의 식별과 그 장소의 보안 취약성을 평가하기 위해 처음에는 사용자의 도움이 필요했지만, 회사라는 장소가 등록된 후부터는 모바일 단말이 회사로 이동하면 방화벽 프로그램 해제, 스크린 세이버의 인증(암호요청)기능 실행, 접근제어 프로그램 및 데이터유출방지 프로그램 실행 등 보안 서비스 재구성을 자동으로 실행하였다.

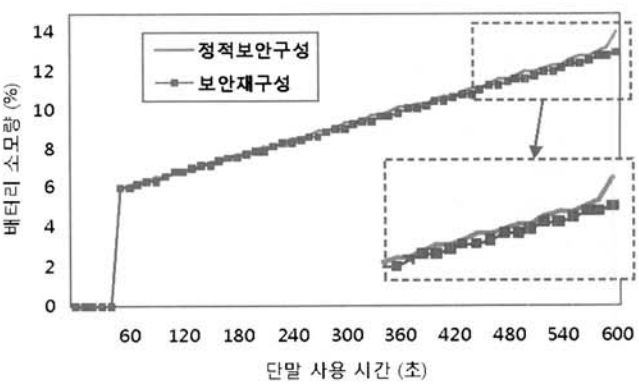
본 논문에서는 자원 효율성관점에서 그 성능을 평가하기 위하여, 본 보안 재구성 프로토타입을 Dell XPS M1710 휴대용 퍼스널 컴퓨터에 설치하고 실험하였다. (그림 5)는 최상의 보안관리 서비스를 제공하는 정적 보안구성 방식과 본 논문에서 제안하는 보안재구성 기법간의 자원 효율성 성능을 비교한 실험이다. 여기서 정적 보안구성방식은 보안상황에 상관없이 휴대용 통신 단말에 있는 모든 보안 기능을 구동하는 방식이다. (그림 5-a)와 (그림 5-b)는 각각 주어진 시간 동안 보안 기능의 총 CPU 점유 시간과 배터리 소모량을 측정한 결과이다. 본 실험에서 휴대용 통신 단말의 집과 회사사이의 왕복주기는 5분으로 설정하였다. (그림 5-a)에서 보듯이, 본 논문에서 제안하는 보안재구성 기법은 보안기능의 CPU 점유 시간에서 정적 보안구성 방식보다 우수하게 나타났다. 본 보안재구성 기법은 정적 보안구성 방식과 비교할 때 보안 기능의 CPU 점유 시간을 약 3/4 으로 줄였다.

일반적으로 CPU 사용 시간은 배터리 소모량과 비례[4]하므로 본 보안재구성 기법이 정적 보안구성방식보다 배터리를 덜 소비한다고 해석할 수 있다. 실제로 배터리 소모량을 측정한 결과, (그림 5-b)에서 보여진 바와 같이 비록 차이는 매우 작지만 본 보안재구성 기법이 정적 보안구성 기법보다 더 적은 배터리를 소모하였다. (그림 5)의 실험결과는 본 논문에서 제안하는 보안재구성 기법이 정적 보안재구성 방식보다 더 적은 컴퓨팅 자원을 사용하며, 따라서 자원 효율성측면에서 더 우수하다는 것을 증명하고 있다.

다음은 보안 재구성기법에서 접속 네트워크 정보와 배터리 상태 등 보안상황정보를 수집하는 작업이 어느 정도의 컴퓨팅 자원을 소모하는지를 분석한 실험이다. (그림 6)은

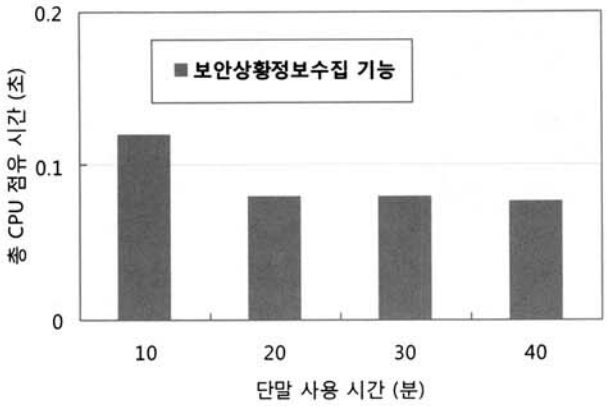


(a) 보안기능의 CPU 점유 시간



(b) 보안기능의 배터리 소모량

(그림 5) 정적보안구성과 보안재구성간의 성능비교
(Fig. 5) Performance comparison between static security configuration and security reconfiguration



(그림 6) 제안된 기법의 부하시험
(Fig. 6) load test of the proposed scheme

(그림 5-(a))의 보안 재구성 실험에서 보안상황정보를 수집하는 작업의 총 CPU 점유 시간을 측정한 실험결과이다. 실험결과, 보안상황정보수집 기능은 CPU의 사용량이 매우 적게 나타났으며 이것은 본 논문에서 제안하는 보안상황정보 수집기능이 휴대용 통신 단말의 성능에 거의 부담을 주지 않는다는 것을 의미한다. 보안상황정보수집 기능의 CPU 점유시간이 단말 사용 시간과 거의 무관하게 결과가 나왔는데, 그 이유는 보안상황정보수집 기능 자체가 일으키는 CPU 부하 양이 보안상황정보수집 기능이 메모리에 처음 로드될 때 일으키는 CPU 부하 양보다도 작을 정도로 매우 적은 수치이기 때문에 실험을 통해 얻은 부하 값의 정확도가 약간 떨어지기 때문이다.

실험을 통하여 본 논문에서 제안하는 보안 재구성 기법은 컴퓨팅 자원을 많이 소비하지 않는 경량급 기법으로써, 사용자 편의성과 자원 효율성측면에서 매우 우수하다는 것을 확인할 수 있었다.

5. 결 론

휴대용 통신 단말은 아직까지는 데스크톱 개인 컴퓨터에 비해 활용도가 떨어지고 있지만, SoC (System on Chop)와 웨어러블 컴퓨팅 등 관련 기술의 발전으로 곧 데스크탑 개인 컴퓨터와 어깨를 나란히 할 것으로 예상되고 있다. 이때 가장 문제가 되는 것이 바로 보안이다. 휴대용 통신 단말은 컴퓨팅자원이 빈약하고 사용자 인터페이스가 불편하기 때문에 데스크톱 개인 컴퓨터에서 사용되는 보안기술을 그대로 수용할 수 없는 문제가 있다.

본 논문에서는 휴대용 통신 단말의 효과적인 보안 관리를 위한 상황인지형 보안재구성 기법을 제안하였다. 제안하는 기법은 휴대용 통신 단말이 위치한 장소의 보안상태와 휴대용 통신 단말이 접속한 네트워크의 보안상태에서 효과가 없는 보안 서비스는 제외하고 반드시 필요한 보안 서비스만을 휴대용 통신 단말에 적용시키는 기술이다. 본 논문에서는 제안하는 보안재구성기법의 프로토타입 시스템 구현하고, 그 성능을 측정하였다. 실험을 통하여 제안하는 기법이 사용자 편의성과 자원 효율성측면에서 매우 우수하다는 것을 확인하였다.

휴대용 통신 단말에서 보안재구성 기법은 크게 수집된 보안상황정보를 기반으로 하여 보안취약성을 평가하는 단계와 보안기능의 능력 및 운용방법을 기술하는 단계로 구분될 수 있다. 후자는 정책기반의 보안관리 등 기존 기술을 사용함으로써 보안관리 자동화를 제공할 수 있다. 그러나 전자의 보안취약성 평가 단계는 자동화가 되려면 평가 정확도를 높이기 위해 더 많은 연구가 필요하다. 또한 위치 정보와 접속 네트워크의 보안관련 정보 등 보안상황 정보를 정확하게 수집하는 것도 이슈중의 하나이다. 센서 등을 이용하여 보안상황정보를 자동으로 수집하여 휴대용 통신 단말의 보안취약성을 자동으로 분석하는 기능은 향후 연구과제로 남긴다.

참 고 문 헌

[1] Ko, S., Ji, Y., Kim, D.: Understanding Influence of Mobile Internet Services on Life Behavior of Mobile Users. In Proc. of Human-Computer Interaction, LNCS, vol. LNCS 4553, pp. 944-953 (2007).

[2] Jamaluddin, J., Zotou, N., Edwards, R.: Mobile phone vulnerabilities: a new generation of malware. In Proc. of IEEE International Symposium on Consumer Electronics, pp. 199-202 (2004).

[3] Mulliner, C., Vigna, G., Dagon, D., Lee, W.: Using Labeling to Prevent Cross-Service Attacks Against Smart Phones. In Proc. of SIG SIDAR Conf. on Detection of Intrusions and Malware & Vulnerability Assessment, LNCS, Vol.4064, pp. 91-108, (2006).

[4] Nash, D. C., Martin, T. L., Ha, D. S., Hsiao, M. S.: Towards an Intrusion Detection System for Battery Exhaustion Attacks on Mobile Computing Devices. In Proc. of the 3rd Int'l Conf. on Pervasive Computing and Communications Workshops, pp.1141-145, (2005).

[5] Martin, T., Hsiao, M., Ha, D., Krishnaswami, J.: Denial-of-Service Attacks on Battery-powered Mobile Computers. In Proc. of the 2th IEEE Annual Conf. on Pervasive Computing and Communications, pp.309-318 (2004).

[6] Jacoby, G. A., Davis IV, N. J.: Battery-Based Intrusion Detection. In Proc. of Globecom 2004, pp. 2250-2255 (2004)

[7] Dey, A. K., Abowd, G. D.: Towards a Better Understanding of Context and Context-Awareness. In Proc. of the workshop on the What, Who, Where, When and How of Context-Awareness (2000).

[8] Schilit, B. N. Adams, N., Want, R.: Context-Aware Computing Applications. In Proc. of IEEE Workshop Mobile Computing Systems and Applications, pp.85-90, (1994).

[9] Chen, G. & Kotz, D. A Survey of Context-Aware Mobile Computing Research. Dartmouth Computer Science Technical Report, TR2000-381 (2000).

[10] Han, L., Jyri, S., Ma, J., Yu, K.: Research on Context-Aware Mobile Computing. In Proc. of 22nd International Conference on Advanced Information Networking and Applications, pp. 24-30 (2008).

안 개 일

e-mail : fogone@etri.re.kr

1993년 충남대학교 컴퓨터공학과(학사)

1995년 충남대학교 컴퓨터공학과(석사)

2001년 충북대학교 컴퓨터공학과(공학박사)

2001년~현 재 한국전자통신연구원 SW 콘텐츠 연구부문 인프라보호연구팀 선임연구원

관심분야 : 컴퓨터 네트워크 및 시뮬레이션, 네트워크 보안, 원격 보안관리, 임베디드 보안

김 기 영

e-mail : kykim@etri.re.kr

1988년 전남대학교 전산통계학과업(학사)

1993년 전남대학교 전산통계학과(석사)

2002년 충북대학교 전자계산학과(박사)

1988년~현 재 한국전자통신연구원 SW 콘텐츠 연구부문 인프라보호연구팀 책임연구원

관심분야 : 네트워크보안, 임베디드 보안 OS 및 복합단말용 보안 기술

서 동 일

e-mail : bluesea@etri.re.kr

1989년 경북대학교 전자공학과(학사)

1994년 포항공과대학교 정보통신공학과(석사)

2004년 충북대학교 전자계산학과(이학박사)

1989년~1992년 삼성전자(주) 연구원

1994년~현 재 한국전자통신연구원 SW 콘텐츠 연구부문 인프라보호연구팀 팀장(책임연구원)

2002년~현 재 ASTAP-Forum 정보보호전문가그룹 의장

1994년~현 재 TTA 정보보호/네트워크 표준화(현 TC5 부의장)

관심분야 : Network, 미래 인터넷, 정보보호(네트워크보안, 해킹 등)