특집 03

UAV 스마트 디바이스 지상 제어 스테이션 사이버 보안 위협 모델

윤종희 (영남대학교)

목 차

1. 서 론

드론 소비 시장에서 기술의 급속한 발전과 및 인기의 증가로 스마트폰 및 태블릿은 우리가 범용시장과 전장에서 드론 운영하는 방식을 변화시키고 있습니다. 자신의 스마트 디바이스를 직장으로 가져 오는 최근의 추세는 미국기업에서 많은 이점을 나타내고 있습니다. 스마트 디바이스는 관련 산업이 비즈니스를 수행하는 방식을 변화시키고 있습니다. 스마트 장치 및 소프트웨어 응용 프로그램을 사용하여 생산성, 이동성, 공동 작업 및 비즈니스 연속성을 향상시킵니다. 그러나 개인용 스마트 장치를 사용하면 해커가 기업의 네트워크 및 개인 데이터에 쉽게 액세스 할 수 있게 해여 많은 보안 취약성이 발생합니다. 이는 회사가 보안 정책을 갖추지 못한 데 따른 결과이,며 네트워크에 연결된 장치를 안전하게 보호하기위한 조치가 필요합니다. 미국 국방부는 과거에 통신에 대한 안전한 연결을 제공 할 수 없는 통신 기술을 항공 제어 기술로 도입하기를 거부했습니다. 다만 이러한 목적으로 사용 가능한 디바이스를 민감한 데이터 [1]의 안전한 처리를 위한 보안 인증 레벨 3을 보유한 블랙 베리(black berry)사의 장치에만 국한하여 허용하였습니다.

그러나 미국 국방부는 최근 스마트폰과 태블릿을 직장과 전장에서 모두 사용 가능하도록 하는 방안을 유연성있게 채택 가능하도록 하였습니다 [2]. 이제 직원들이 스마트폰을 사용하면 현재 블랙 베리 휴대폰으로 액세스 할 수 없는 애플리케이션에 액세스 할 수 있습니다. 군사 서비스는 스마트 장치를 전쟁터로 전환하여 테러와의 전쟁에서 수백만 달러의 무인 항공기를 제어하기 위한 소형 장치로 군인에게 추가적인 기능과 기능을 제공할 수 있습니다. 그러나 국방부는 전장에서 기술의 관련성을 유지하기 위해 보안 위협 평가가 수행되거나 보호 조치가 취해지지 않을 때 사이버 보안 위협 및 취약점으로부터 자

산을 보호하지 못할 수도 있습니다. 우리는 UAV의 휴대형 지상 제어 스테이션(Ground Control Station, GCS)으로 안드로이드 및 애플 스마트 장치를 사용할 때 가능한 위협 모델을 여기서 살펴보겠습니다. 안전하지 않은 모바일 장치를 사용하면 UAV 도용 및 기밀 정보의 무단 공개가 발생할 수 있습니다. 지능형 장치 지상 관제소에 대한 사이버 보안 공격은 전장에서 위험하며 공격의 결과는 심각합니다. 군은 위협 환경을 이해하고 적절한 보안 대책이 개발되고 구현되도록 하기 위해 위협 모델 및 위험 평가를 진행해야 합니다.

2. 무인 항공기 공격과 동기

UAV에 대한 몇 가지 사이버 보안 공격은 보안 평가가 부족하고 보안 대책이 부적절하기 때문에 지난 수년 간 발생했습니다. UAV에 대한 최초의 공개 공격은 2009년에 발생하였으며 이라크 무장 세력은 프레데터 드론 (Predator drones)에서 사용하는 보안되지 않은 통신 링크에서 라이브 비디오 피드를 가로 채기 위하여, 당시 $26에 판매되는 SkyGabber 소프트웨어를 사용하였습니다 [3]. 2011 년 10월, 이동식 하드 드라이브를 사용한 이후 프레데터 (Predator) 및 리퍼 (Reaper) 지상 제어 스테이션에서 키 로깅 악성코드가 발견되었습니다. 이 바이러스는 주변의 다양한 컴퓨터로 확산되었지만 다행스럽게도 UAV 작업을 방해하지 않았고 권한이 없는 사람에게 민감한 정보를 유출하지도 않았습니다[4]. 미국의 RQ-170 Sentinel UAV는 2012 년 12월에 아프가니스탄 국경에서 이란 정부에 의해 납치되었습니다. 이란 정부는 임무 및 유지 관리 데이터를 포함한 민감한 데이터를 얻기 위해 UAV를 성공적으로 착륙시킬 수 있었습니다 [5]. 최근에 텍사스 대학은 2012 년 7월에 국토 안보부와 협력하여 위성 위치 확인 시스템 (GPS)을 위장하고 UAV를 완전히 통제하기 위해 1000 달러 상당의 장비를 사용하여 군사용 무인 항공기를 납치 할 수 있는 능력을 보여주었습니다 [6].

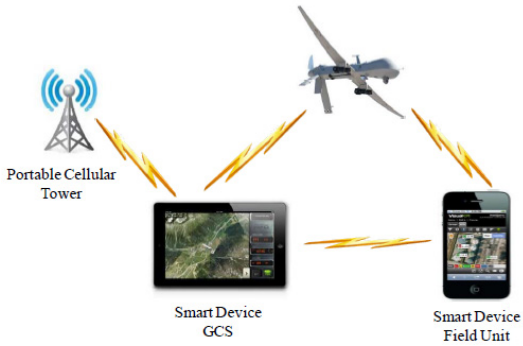
블랙베리가 보안 기능을 개선하였음에도 불구하고 스마트 디바이스 시장의 점유율은 5%에 머물고 있습니다. 91.1%의 사용자는 애플 혹은 안드로이드 디바이스를 사용하고 있으며 안드로이드가 스마트 디바이스 시장을 이끌고 있습니다. 스마트 기술의 급속한 발전과 장치의 인기로 미국방부는 전장에서 사용하기 위해 Apple 및 Android 스마트 장치를 조달 할 계획을 발표했습니다[1]. 상용으로 사용가능한 스마트 디바이스는 군사용의 견고한 디바이스와 비교하여 최신의 기술로 합리적인 가격을 갖추었습니다. 군사용으로 특화된 견고한 장치는 종종 수년간의 개발로 인하여 상용화된 스마트 디바이스에 비하여 열배가 넘는 높은 가격을 갖기도 합니다. 상업용 스마트 장치를 조달하기 위한 비용 절감 외에도 소비자 시장에서 Apple 및 Android 스마트 장치의 인기는 개인 생활에서 이러한 동일한 장치를 사용하는 군인에 대한 사용 편의성 교육 비용을 최소화하는 것과 같습니다.

이러한 스마트 장치는 여러 목적으로 모든 군대에서 테스트되었습니다. 전장에서 스마트 장치를 사용하려면 스마트 장치, 소프트웨어 응용 프로그램 및 군인이 응용 프로그램을 안전하게 다운로드 할 수 있게 해주는 소프트웨어 응용 프로그램 데이터베이스를 관리하고 보안을 유지하기 위한 보안 통신 네트워크를 개발해야합니다. 미국 국방부는 방위 산업에 진출하여 최대 800만대의 Apple 및 Android 스마트 장치를 처리하고 보안유지 통신하는 안전한 통신 시스템을 구축하고 있습니다[7]. 정부 기관은 방위 산업과 함께

현재 보안 소프트웨어 응용 프로그램 데이터베이스와 군용 소프트웨어 응용 프로그램 전장 응용 프로그램을 개발하고 있습니다.

2.1 UAV 스마트 디바이스 지상 제어 스테이션

UAV는 센서, 통신, 임베디드 제어 기술 및 기술의 소형화의 급속한 발전으로 인해 크게 인기를 얻었습니다. 오늘날 UAV를 50 개국 이상이 군대에 도입했습니다. 미국은 혼자서 국방부 (DOD) 항공기의 40 퍼센트 이상을 구성하는 7,500 개 이상의 무인 항공기를 운영합니다. (Blackhurst, 2012) UAV는 주로 감시, 정보 및 정찰 임무를 위해 군사 임무를 지원하는 데 사용됩니다. UAV 지상 관제소는 임무 수행에 중요합니다. UAV는 전장에서 또는 근처에서 UAV를 제어 및 모니터링하며 통신의 중심 노드입니다. 지상 제어 스테이션 (GCS)은 UAV에서 수집된 정보를 수신하고 데이터를 처리하며 네트워크의 다른 사용자에게 데이터를 제공합니다. 고정식 GCS는 대형 UAV용 이동식 트레일러 내에 광범위한 하드웨어 및 개인용 컴퓨터 워크스테이션 설치로 구성되는 경우 비용이 많이 소요되는 경우가 있습니다. GCS는 조종사에게 UAV를 조작하고 페이로드 운영자가 컴퓨터 시스템을 조작하고 지능을 수집하며 UAV의 정보를 전장의 다른 최종 사용자에게 전달하도록 요구합니다. 소형 무인 공중 차량 (SUAV)은 일반적으로 휴대용 지상 관제소를 사용하여 통제되고 감시됩니다. 핸드 컨트롤러, 견고한 노트북, RF 트랜시버 장치 및 컨트롤러 상자로 구성되어 있습니다. 핸드 컨트롤러를 사용하는 작업자는 SUAV의 카메라에서 스트리밍 비디오로 SUAV를 조작하고 다른 운영자는 랩톱을 사용하여 인텔리



(그림 1) 스마트 장치 GCS 네트워크 구성도

전스 데이터를 수집하고 분석하여 전투 현장의 다른 최종 사용자에게 보급합니다. 지상 관제소는 UAV와 GCS 사이 및 GCS와 전장 네트워크의 최종 사용자간에 안전한 통신 연결을 가져야 합니다. 국방부는 기존의 지상 관제소의 기능을 활용하여 실시간 항법 장비 비행 디스플레이, 네비게이션 시스템, 시스템 상태 모니터링 및 사전 진단 디스플레이, 그래픽 이미지 및 위치를 제공하기 위해 소프트웨어 앱을 사용하여 모바일, 휴대용 스마트 장치로 소형화했습니다. 스마트 장치는 또한 군인이 UAV 카메라를 조종하여 목표물과 적을 발견하고 위치 및 시간과 함께 비디오 데이터를 다른 병사들과 공유하여 목표에 관한 신속한 결정을 내릴 수 있게 해야 합니다.

3. 위협 모델 (THREAT MODEL)

스마트 장치 GCS의 위협 모델 분석은 스마트 장치 GCS 네트워크 내의 보안 위협 및 예방 대책을 식별하는 것이 중요합니다. NIST (National Institute of Standards and Technology)는 연방 정보 보안 관리법 (Public Information Security Management Act, Public Law 107-347)에 따라 정보 보안 표준 및 지침을 개발하는 지정된 기관입니다. NIST의 위협 모델링 정의에는 관심있는

리소스와 해당 리소스와 관련된 가능한 위협, 취약성 및 보안 제어를 식별한 다음, 성공적인 공격 및 영향의 가능성을 계량화하고, 마지막으로 이러한 정보를 분석하여 보안 제어를 개선해야 할 모듈을 결정해야합니다. 위협 모델링에 대한 NIST의 정의를 사용하여 제안된 위협 모델은 공격의 관심과 동기, 스마트 장치 기지국의 공격 진입점, 사이버 보안 취약성 및 스마트 보안을 향상시키는 단계의 네 가지 주요 구성 요소를 분석해야 합니다. BlackBerry 스마트 장치는 현재 연방 정보 처리 표준 인증을 충족하는 유일한 스마트 장치이므로 미국 정부에서 사용하기에 적합한 것으로 간주되어 위협 모델에서 분석하지 않습니다. 위협 모델은 UAV 응용 프로그램을 위한 Apple 및 Android 스마트 장치의 사이버 보안 취약점에 중점을 두었습니다.

스마트 디바이스 지상 스테이션에 대한 공격 목표는 1) UAV의 제어를 막기 위해 장치의 작동을 방해하고, 2) UAV를 제어하기 위해 스마트 장치 지상 관제소의 제어권을 얻고 3) 데이터에 대한 액세스 권한을 얻어 공격자에게 제공합니다. 성공적인 공격에는 정보 보안 목적 중 하나 이상 (기밀성, 무결성 또는 가용성)의 상실이 요구됩니다. 기밀성 상실은 전송 및 저장된 데이터의 무단 공개입니다 [8]. 기밀성에 대한 가장 일반적인 위협 중 하나는 통신 네트워크를 도청하는 것입니다. UAV는 주로 감시, 정보 및 정찰 임무를 위한 군사 임무를 지원하는 데 사용됩니다. 기밀 유지가 실패하면 임무를 위태롭게하고 생명을 위협 할 수 있습니다. 무결성의 손실은 전송 및 저장된 데이터에 대한 고의 또는 의도하지 않은 변경입니다. 악성코드는 사용자의 지식 없이 소프트웨어를 수정하여 민감한 정보에 액세스하거나 심지어 원격으로 지상 제어 스테이션을 완전히 차지할 때 사용됩니다. 가용성의 손실은 필요할 때마다 모바일 장치를 사용하여 리소스에 액세스하는 기능의 손실입니다. 통신 네트워크는 재밍 장치를 이용하여 GCS 네트워크 허브의 끝단 장치와 UAV의 통신을 불가능하게 할 수 있습니다.

3.1 취약성

UAV 지상 스테이션은 정보, 감시 및 정찰 임무에서 데이터 통신의 핵심 노드이기 때문에 매우 중요합니다. GCS는 UAV를 조종하는데 사용될 뿐만 아니라 UAV에서 이미지, 비디오 및 데이터를 수신하여 이러한 정보를 지상군 및 기타 기관에 제공합니다. 공격자가 스마트 디바이스 지상 제어 스테이션의 서비스를 제어하거나 해제하거나 중단하면는 방식으로 임무 완수를 방해 할 수 있습니다. 지상 제어 스테이션에 대한 성공적인 공격은 하드웨어, 소프트웨어 (운영 체제 및 소프트웨어 응용 프로그램) 및 통신 네트워크를 이용하여 수행될 수 있습니다. 아래에서는 스마트 디바이스 UAV 지상 제어 스테이션의 취약점과 위협에 대해 설명합니다.

3.1.1 하드웨어 취약성

카메라, 가속도계, 마이크 및 GPS와 같은 스마트 장치 내의 센서라고도 하는 하드웨어 리소스에는 공격자가 최종 사용자의 위치를 모니터링, 탭 또는 식별하는데 사용할 수 있는 중요한 정보가 포함될 수 있습니다. 이러한 취약점은 아래 명시된 운영 체제 또는 소프트웨어 응용 프로그램의 다른 소프트웨어 취약점을 통해 입력된 악성 소프트웨어 및 공급망 사이버 보안 위험을 통해 침입할 수 있습니다. 공급망 사이버 보안 위험은 정보 기술 시스템에 의도적으로 스파이웨어를 설치하거나 추후에 정부와 대기업에 판

매되는 악의적인 펌웨어가 있는 회로를 변경하는 적대적인 원인에 의해 발생됩니다 [9]. 전자 구성 요소가 네트워크에 연결되면 적이 네트워크에 쉽게 접근 할 수 있게 되거나, 전자 장치의 획득한 제어가 악용되어 해를 입히거나 해를 입힐 수 있습니다. 많은 공급 업체가 다국적 기업이며 다른 회사와의 합병으로 인해 기업 소유권을 채택하거나 공급망 보안을 통제하는 것이 사실상 불가능합니다.

스마트 디바이스의 지상 제어 스테이션 하드웨어에 대한 위협에는 배터리 고갈, 범람, 감시 및 USB 공격이 포함됩니다. 배터리 고갈 공격으로 인해 배터리가 평소보다 빨리 방전되어 스마트 장치를 죽이고 궁극적으로 군인이 UAV를 제어하거나 정보를 보급하지 못하게 합니다. 침수 공격은 수많은 문자 메시지 또는 수신 전화로 장치에 과부하가 걸리므로 군인이 UAV를 제어하거나 네트워크 정보를 제공하거나 받지 못하게 함으로써 스마트 장치를 비활성화합니다. 감시 공격은 스마트 장치 리소스/센서를 원격으로 사용하여 통신 및 군인 이동을 모니터링하므로 공격자가 UAV 및 주변의 다른 군인을 조종하는 위치를 식별하여 물리적 공격의 위험에 처하게 합니다. 마지막으로, USB 공격은 USB 연결로 수행된 스마트 장치의 동기화 및 데이터 백업을 활용합니다. USB 연결은 악성 소프트웨어를 네트워크로 전송하고 네트워크에 대한 가시성과 액세스를 허용합니다.

3.1.2 소프트웨어 취약성

Apple iOS는 Apple에서 개발하고 배포하는 운영 체제입니다. 소프트웨어에 대한 모든 변경 사항 및 업데이트는 스마트 장치의 보안을 강화하기 위해 Apple에서 최종 사용자에게 직접 관리됩니다. 그러나 애플 스마트 디바이스는 사용자가 자신의 재량에 따라 디바이스를 커스터마이징하고 소프트웨어 애플리케이션을 설치할 수 있도록 제한 및 보안 조치를 제거 할 수 있는 “jailbroken” 기능을 사용할 수 있습니다. Apple iOS 운영 체제에서 실행되는 모든 소프트웨어 응용 프로그램은 Apple 사양을 충족해야하며 승인된 개발자가 디지털 서명해야합니다. 소프트웨어 응용 프로그램은 Apple 스토어를 통해서만 배포할 수 있습니다. Google Android는 보안 조치가 가장 적은 인기있는 운영체제입니다. Android는 공개 운영 체제이므로 다양한 스마트 장치 유형 및 통신 사업자의 요구 사항을 충족시키기 위해 소프트웨어 코드를 공개적으로 사용할 수 있습니다. 개방형 운영체제로 인해 Android 스마트 폰 및 장치의 다양한 변형이 발생하여 동일한 휴대 전화를 사용하는 여러 이동 통신사마다 운영 체제 소프트웨어의 변형이 다를 수 있습니다. 소프트웨어 업데이트는 지루한 과정이므로 일부 전화기는 업데이트를 수신하고 다른 전화기는 그렇지 않을 수 있습니다. Google 업데이트는 이동 통신사 및 타사 응용 프로그램 개발자의 재량에 따라 최종 사용자에게 푸시됩니다. 캐리어 또는 타사 소프트웨어 개발자는 스마트 장치에 대한 취약성이 증가하는 최종 사용자에게 업데이트를 푸시하기를 거부 할 수 있습니다.

Android 소프트웨어 응용 프로그램은 해당 동작을 담당하는 개발자가 디지털 서명해야합니다. 소프트웨어 앱은 Google Play 및 타사 애플리케이션 마켓 플레이스를 통해 배포 할 수 있습니다. Google Android를 사용하면 누구나 품질이나 보안 테스트없이 Google Play에서 다운로드 할 수 있도록 앱을 제출할 수 있으므로 사이버 보안 취약성이 소프트웨어 데이터베이스 및 Android 기기에 쉽게 악화됩니다. 모바일 운영 체제는 스마

트 장치의 핵심이며 하드웨어 리소스와 소프트웨어 응용 프로그램을 제어합니다. 운영 체제에 침투하면 공격자는 모든 하드웨어 리소스와 소프트웨어 응용 프로그램을 완벽하게 제어 할 수 있습니다. 운영 체제를 제어하면 공격자가 하드웨어 리소스를 조작하고 스마트 장치가 이미지 및 비디오를 캡처하고 대화를 녹음하고, 중요한 정보를 보고대상이 되는 개인의 위치를 파악할 수 있는 모니터링 장치를 만들 수 있습니다. 소프트웨어 응용 프로그램은 스마트 장치 지상 제어 스테이션의 기능에 중요하여 실시간 항공 전자 디스플레이 비행, 네비게이션 시스템, 시스템 상태 모니터링 및 사전 진단 디스플레이, 그래픽 이미지 및 위치 매핑 및 UAV를 제어 및 작동하기 위한 내부 데이터 처리 기능을 제공합니다. 소프트웨어 응용 프로그램에 대한 성공적인 공격은 공격자가 UAV 기능을 제어하고 UAV에서 수집 한 데이터에 액세스하여 대상자를 신체적 위험에 빠뜨릴 수 있습니다.

모바일 장치의 운영 체제는 개인용 컴퓨터의 운영 체제를 유사하므로 개인용 컴퓨터에서 흔히 볼 수 있는 보안 위협과 같은 것을 스마트 장치에서 볼 수 있습니다. 악성 코드는 장비를 중단 시키거나 민감한 정보를 수집하거나 장비를 제어하는 데 사용할 수 있습니다. 스마트 장치에서 발견되는 일반적인 악성코드는 트로이 목마, 봇넷, 웜, 키 로거 및 루트킷이 있습니다. 이러한 악성코드는 운영 체제 소프트웨어를 액세스 할 수도 있습니다. 소프트웨어에 대한 다른 위협으로는 피싱 및 데이터 유출이 있습니다. 피싱 공격은 네트워크에 신뢰할 수 있는 당사자로 가장하여 중요한 정보에 액세스 할 수 있게합니다. 이러한 유출 정보는 중요한 데이터의 무단 전송으로 이어질 수 있습니다.

3.1.3 통신 네트워크 취약성

스마트 디바이스형 지상 제어 스테이션이 기능을 수행하려면 통신 네트워크가 필요합니다. 전술 군사 환경에서 대부분의 무선 네트워크는 고정된 기지국 또는 이동 가능한 기지국, 고 대역폭 유선 네트워크 백본으로 설정됩니다. 전장 환경에서 고정 기지국은 매력적인 표적이며 공격에 매우 취약합니다. 정지된 기지국의 파괴는 통신 네트워크를 방해하게 될 것이다. 이러한 상황이 발생하면 병사들은 보안 무선 네트워크상에 있지 않을 수도 있는 통신을 계속하기 위해 상용 무선 네트워크를 만들거나 상용 네트워크를 이용하여 그들이 지원하는 통신 네트워크, 부착된 장치 및 임무에 취약점을 발생하게 됩니다. 통신 네트워크에 대한 공격은 UAV와 스마트 장치 지상 제어 스테이션 간의 연결을 방해하고 UAV의 작동 및 제어를 방지하고 GCS 네트워크 허브의 다른 최종 사용자간에 정보를 유출하여 임무 완료를 방해 할 수 있습니다. 네트워크 및 장치에 대한 공격은 UAV 감시임무에서 수집된 정보가 무단으로 공유 될 수 있으므로 적절한 대응이 필요합니다. 통신 네트워크에 대한 위협으로는 네트워크 도청, 스푸핑, 서비스 거부 및 재밍이 있습니다. 네트워크 도청 또는 스니핑은 네트워크를 통해 전송되는 패킷을 캡처 및 해독하는 방식으로 발생합니다. 스푸핑은 침입자 또는 소프트웨어가 거짓 데이터를 사용하여 네트워크에 액세스 할 수 있게 합니다. 서비스 거부 또는 네트워크 정체로 인해 GCS 허브 네트워크의 링크 또는 노드가 광범위한 양의 데이터로 오버로드되어 네트워크 성능의 저하 또는 서비스 거부가 발생할 수 있습니다. 마지막으로, 재밍 장치는 네트워크의 다른 구성 요소뿐만 아니라 스마트 장치 GCS와 UAV 간의 통신을 방해 할 수 있으

〈표 1〉 GCS 위협 모델

	하드웨어 취약성				소프트웨어 취약성			통신 네트워크 취약성			
	배터리 고갈	범람	감시	USB	악성코드	피싱	데이터유출	도청	스푸핑	서비스거부	재밍
신뢰성			X	X	X		X	X	X		
무결성			X	X	X	X			X		
가용성	X	X			X	X				X	X

므로 UAV의 제어와 네트워크 허브 내의 정보 제공을 방해할 수 있습니다.

4. 결 론

우리는 스마트 디바이스를 휴대 가능한 UAV 지상 제어 스테이션으로 사용하려는 흐름에 따라 이와 관련된 보안 취약성을 살펴보았습니다. 위협 모델은 UAV 스마트 디바이스 GCS의 위협 프로필을 분석하기 위해 개발되었습니다. 이것은 스마트 디바이스 하드웨어, 소프트웨어 및 통신 네트워크 내의 취약점에 중점을 둡니다. 요약하면 하드웨어에 대한 위협은 주로 훼손된 장치에 대한 물리적 연결과 소프트웨어 응용 프로그램 및 네트워크 연결의 악성 코드를 통해 발생합니다. 스마트 장치 하드웨어 리소스는 군인의 통신 및 이동을 모니터링하기 위해 악성코드에 의해 조작 될 수 있습니다. 소프트웨어 운영 체제 및 소프트웨어 응용 프로그램은 UAV 스마트 장치 GCS의 기능에 중요합니다. 소프트웨어가 악성 코드 위협으로부터 적절히 보호되지 않으면 결과가 심각 할 수 있습니다. 운영 체제의 정기적인 업데이트 및 바이러스 백신 소프트웨어로 보호해야 합니다. 소프트웨어 응용 프로그램은 취약점에 대해 테스트를 거쳐 정기적으로 업데이트되어 보안을 보장해야만 할 것입니다. 통신 네트워크는 취약점의 주요 영역이며, 이 영역의 결함으로 인하여 소프트웨어 및 하드웨어 취약성 내에서 식별된 많은 공격이 발생할 수 있습니다. 네트워크의 가용성은 원격 위치의 전장 운영에 대한 주요 관심사이며 현장에서 가장 큰 공격대상 중 하나입니다.

참 고 문 헌

[1] Dalton, W., “RIM's BlackBerry phones may lose public sector monopoly,” Retrieved 5/24/13, 2013, from http://www.itproportal.com/2012/08/24/rims-blackberry-phones-maylose- public-sector-monopoly-/, 2012.

[2] McGarry, B., “Pentagon Will Open Networks to Apple, Google Devices in 2014,” Retrieved 3/21/13, 2013, from http://www.bloomberg.com/news/2013-02-26/pentagon-will-opennetworks-to-apple-google-devices-in-2014.html, 2013.

[3] Gorman, S., et al., “Insurgents Hack U.S. Drones,” The Wall Street Journal, WSJ.com, 2009.

[4] Nguyen, T. C., “Virus attacks military drones, exposes vulnerabilities.” Retrieved from http://www.smartplanet.com/blog/thinking-tech/virus-attacks-militarydrones- exposes-vulnerabilities/8858, 2011.

[5] Paganini, P., “Hacking Drones Overview of the Main Threats,” Retrieved from http://resources.infosecinstitute.com/hacking-drones-overview-of-themain-threats/, 2013.

[6] Nguyen, T. C., “How college students hijacked a government spy drone,” Retrieved from http:/

/www.smartplanet.com/blog/thinking-tech/how-college-studentshijacked- a-government-spy-drone/12214, 2012.

[7] Munoz, C., "Report: DOD opens door to Apple, Android-built systems," Retrieved from http://thehill.com/blogs/defconhill/ industry/265395-report-dod-opens-door-to-apple-android-builtsystems, 2013.

[8] Oh, T., et al., "Best security practices for android, blackberry, and iOS," Enabling Technologies for Smartphone and Internet of Things (ETSIoT), 2012.

[9] Goodwin, B., "IT manufacturers fight cyber espionage risks in the supply chain," Retrieved from http://www.computerweekly.com/news/2240181320/IT-manfucturerstackle-cyber-espionage-risks-in-the-supply-chain, 2013.

저 자 약 력

윤 종 희

이메일 : youn@yu.ac.kr

- 2003년 경북대학교 전자전기공학부 (학사)
- 2011년 서울대학교 전기컴퓨터공학부 (박사)
- 2011년~2012년 강릉원주대학교 컴퓨터공학과 강의전담교수
- 2012년~2013년 한국전자통신연구원 부설연구소 연구원
- 2013년~현재 영남대학교 컴퓨터공학과 조교수
- 관심분야 : 사이버 보안, 컴파일러, 소프트웨어 최적화, 임베디드 시스템