스마트워치를 이용한 원자력발전소 제어시스템 공격 가능성 연구

김태희

한국원자력통제기술원

kimtaehee@kinac.re.kr

A Study on the Possibility of Attacking Nuclear Power Plant Industry Control Systems using Smart Watches

Kim Taehee

Korea Institute of Nuclear Nonproliferation and Control

요 약

최근 원자력발전소의 제어시스템들이 디지털화 되면서, 이에 대한 사이버 위협이 지속적으로 증가하고 있다. 원자력안전위원회는 증가하는 사이버 위협에 대응하기 위하여, '14년 11월부터 국내 원자력 발전소가 일정 수준 이상의 사이버보안 체계를 갖추도록 규제하고 있다. 이러한 규제는 원자력발전소의 안전, 보안, 비상대응 기능에 필요한 주요 디지털자산이 외부 공격에 노출되는 것을 원천적으로 차단하거나, 최소화하는 내용을 포함하고 있다. 그러나 출입자가 착용한 스마트워치는 스마트폰, 노트북 및 휴대용 저장매체(USB)와 같은 잘 알려진 공격 수단 대비, 시계와 비슷한 외형으로 인해 사전에 확인하고 통제하기 어려워, 디지털자산에 대한 사이버공격에 활용될 가능성이 있다. 본 논문에서는 스마트워치가 가진 특성과 이로 인한 위협 및 관련 규제, 마지막으로 스마트워치 위협에 대응하기 위한 향후 과제를 알아본다.

Ⅰ. 서 론

원자력발전소 제어시스템에 있어, 기존의 아날로그 시스템을 대신하여 운영과 관리에 이점이 있는 디지털 제어시스템의 비중이 점점 높아지고 있다. 국내에서도 최초 '78년에 상업운전을 시작한 고리 1호기 이래, 한국형 표준원자로인 OPR-1000과 그 개량형인 APR-1400에 이르기까지 제어시스템은 꾸준히 디지털화 되어 왔다.

제어시스템의 디지털화에 비례하여 제어시스템에 대한 사이버 위협 역시 지속적으로 증가해 왔다[1][2]. 이에 대응하기 위하여 우리나라는 '14년 11월부로 "물리적방호규정등의 작성내용의 항목별 세부작성 기준"[3]에 기존의 물리적 공격에 대한 내용 외에 사이버 공격을 의미하는 "전자적 침해행위"를 명시적으로 추가하고, 이에 대한 규제를 시행하였다.

국내 원자력 안전 및 안보 규제 기관인 원자력안전위원회는 구체적인 규제의 시행을 위해 안보 업무의 위탁기관인 한국원자력통제기술원으로 하여금 KINAC/RS-015[4] 등 구체적인 심·검사기준을 마련하도록 하였다. 원자력발전소는 규제기준에 따라 안전, 보안, 비상대응 등의 주요 기능을 수행하는 제어시스템 등을 필수디지털자산으로 식별하였으며, 이들이 외부 공격에 노출되는 것을 원천적으로 차단하거나, 노출되더라도 공격의 영향을 최소화할 수 있도록 보호 체계를 운영 중에 있다.

그러나 그 위험성이 이미 잘 알려진 노트북, 스마트폰, USB 등의 휴대용 저장매체와는 달리, 최근 일상화(23년 1월 기준 보급율 8.9%[5]) 되기 시작한 스마트워치의 사이버 위협에 대해서는 연구가 필요한 상황이다.

Ⅱ. 스마트워치로 인한 사이버 위협 분석

1. 기존 스마트워치에 의한 사이버 위협

기존의 스마트워치는 스마트폰과 연계하여 그 기능을 확장하거나, 건강 정보 등을 기록할 목적으로, 애플워치[6], 갤럭시워치[7]와 같이 하나의 완성된 제품으로 제공되는 경우가 일반적이었다. 이러한 스마트워치들은 사용자의 데이터를 보호하기 위하여, 보안 시동 및 보안 소프트웨어 업데이트 수행, 운영 체제 무결성 유지, 데이터 암호화, 분실 시 원격 초기화, 암호 설정 등의 기능을 제공한다.

그러나 스마트워치의 아래 표1과 같은 통신 기능들과 악성코드가 설치될 수 있는 내·외부 메모리 등은 스마트워치가 다양한 사이버 공격 벡터에 노출되어 있고 또한 위·변조될 수 있음을 시사한다. 실제로 애플워치 운영체제인 watchOS의 '23년 이후 발표된 취약점은 154개에 달하며, 그 중에는 CVSS 점수가 9점을 넘는 취약점도 6개 포함되어 있다[8]. 아직까지 발견되거나 알려지지 않은 취약점까지 고려한다면, 스마트워치에 의한 사이버 위협은 반드시 원자력발전소의 사이버보안 체계에 반영되어야 한다.

	애플워치 울트라 2[6]	갤럭시워치 6 클래식[7]
운영체제	watchOS 10	Wear OS
프로세서	Apple S9 + W3	삼성 엑시노스 W903 SOC
메모리	64GB 내장	18GB 내·외장
입력방식	터치스크린 등	터치스크린 등
통신기능	4G, 3G, Wi-Fi, 블루투스, NFC, UWB	4G, 3G, Wi-Fi, 블루투스, NFC, UWB

표 1 기존 스마트워치의 공격 벡터

2. 프로그래밍 가능한 스마트워치에 의한 사이버 위협

최근 일부 제조사들은 다양한 하드웨어 조합으로 이루어져 있으며,

사용자로 하여금 필요에 따라 그 기능을 프로그래밍 할 수 있는 DIY(Do It Yourself) 형태의 스마트워치들을 제공하고 있다. 이들은 아두이노[9]와 같은 보드를 기반으로, 공통적으로 사용자 프로그램의 다운로드와 저장을 위한 인터페이스와 내·외장 메모리를 갖추었다는 특징을 공유한다. 아래 표2는 인터넷 검색을 통해 쉽게 구매 가능한 DIY 형태의 스마트워치 중 일부이다.

T-Watch[10]	Watchy[11]	Deauther Watch[12]
		

표 2 시판 중인 DIY 형태의 스마트워치

이들 스마트워치를 이용한 가장 쉬운 위협은, 사용자의 프로그래밍 인터페이스를 통해 필수디지털자산에 스마트워치를 휴대용 저장매체로 연결하여 악성코드를 주입하거나, 로그 데이터 등을 위·변조하는 것이다. 실제로, 표2에 제시된 Deauther Watch는 제품 상세 페이지에 Bad USB로 작동 가능하다는 점까지 명시적으로 제시하고 있다. 다만 그 외관이 완성품으로 보기는 어려우나, 외형을 3D 프린트하여 보다 시계에 가까운 외형으로 위장할 수 있을 것이다.

다른 위협으로는 스마트워치의 칩셋이 GPIO(General Purpose Input /Output) 기능을 제공한다면 이를 활용하여 제어시스템의 입·출력신호에 직접 혹은 전압/전류 조정회로를 통해 연결하는 것이 있다. 이러한 공격을 성공적으로 수행한다면 원자력발전소의 각종 변수를 참에서 거짓으로 혹은 그 반대로 교란할 수도 있다.

Ⅲ. 스마트워치 위협에 대응하기 위한 사이버보안 이행

원자력발전소 관련 심·검사기준인 KINAC/RS-015에 따르면, 필수디지털자산에 영향을 주거나, 직·간접적으로 연결되지 않는 자산일지라도, 이러한 자산들에 대한 사용제한 절차를 수립 및 이행하도록 요구하고 있다. 예를 들어 원자력발전소는 필수디지털자산에 연결될 가능성이 있는 휴대용 매체 및 모바일 기기의 사용을 제한하기 위한 절차를 수립 및 이행하여야 한다. 이에 따라, 원자력발전소에 반입되는 휴대용 매체 및 모바일 기기는 여러 가지 방법으로 검색을 거치게 된다.

그러나 II.1에서 살펴본 위·변조된 스마트워치의 반입을 사전에 적발하기란 어려우며, II.2에서 살펴본 DIY된 스마트워치 역시 그 외형이 다소 특이한 경우라 할지라도, 외관 검사나 엑스레이 검사만을 통해서는 마치 정상적인 스마트워치처럼 기판만 식별될 뿐이므로 서로간의 구분이 어려울 수 있다.

물론 KINAC/RS-015는 필수디지털자산에 대한 기술적, 운영적, 관리적 측면에서 다양한 조치에 의한 사이버보안 심층 방호를 요구하고 있으므로, 이를 준수한다면 스마트워치만으로 원자력발전소의 전체 보안 조치를 무력화할 수 있을 가능성은 매우 낮다. 하지만 위협의 최소화라는 측면에서 스마트워치의 위협에 대한 원자력발전소의 대응 필요성은 앞으로 점점 더 증가할 것이다.

Ⅳ. 결 론

본 논문에서는 스마트워치의 특성과 이로 인해 발생할 수 있는 위협을 살펴보았다. 향후 스마트워치의 기능은 점점 더 고도화 될 것이며, 스마트워치로 인한 위협 역시 점점 더 증가할 것이다. 이에 대응하기 위해서는 최신 기술과 동향을 반영한 보안 대책의 마련과 함께 무엇보다도 원자력발전소 근무자의 보안 인식 제고가 필요할 것으로 판단된다. 기술은 빠르게 발전하고 있으며, 규제가 요구하는 사항만을 글자 그대로 준수한다는 인식으로는 스마트워치와 같은 새로운 위협에 대응할 수 없을 것이다.

ACKNOWLEDGMENT

This work was supported by the Nuclear Safety Research Program through the Korea Foundation Of Nuclear Safety(KoFONS), granted financial resource from the Nuclear Safety and Security Commission (NSSC), Republic of Korea. (No. 2106012)

참 고 문 헌

[1] Frost & Sullivan, “Asia-Pacific Industrial Control Systems Security Market,” Nov. 2015.,

[2] 동아사이언스, “SMR 등 원전 확대...“방심할 수 없는 원전 사이버 공격,” Apr. 2023.(http://m.dongascience.com/news.php?idx=59158),

[3] 원자력안전위원회, “물리적방호규정등의 작성내용의 항목별 세부작성기준,” Nov. 2014.,

[4] 한국원자력통제기술원, “KINAC/RS-015(Rev.2) 원자력시설의 컴퓨터 및 정보시스템 보안,” Dec. 2023.,

[5] 방송통신위원회, “2022년 방송매체 이용행태 조사,” p. 78, Jan. 2023.,

[6] 애플워치 울트라 2, https://namu.wiki/w/Apple%20Watch%20Ultra%202Encryption

[7] 갤럭시워치 6 클래식, https://namu.wiki/w/갤럭시%20워치6%20클래식

[8] Apple Watchos : Security Vulnerabilities, CVEs, https://www.cvedetails.com

[9] 아두이노, https://www.arduino.cc

[10] LILYGO TTGO T-Watch, https://www.lilygo.cc

[11] Watchy, https://watchy.sqfmi.com

[12] DSTIKE Deauther Watch V4S, https://dstike.com