JDCS
디지털콘텐츠학회논문지
Journal of Digital Contents Society
Vol. 22, No. 7, pp. 1135-1141, Jul. 2021

Check for updates

디지털 사이니지 콘텐츠 보안 필요성에 관한 연구

이 재 웅[1] · 소 우 영[2*]
[1]한남대학교 컴퓨터공학과 박사과정
[2*]한남대학교 컴퓨터공학과 교수

A Study on the Need for Digital Signage Content Security

Jae-Ung Lee[1] · Woo-Young Soh[2*]

[1]Doctor's Course, Department of Computer Engineering, Hannam University, Daejeon 34430, Korea
[2*]Professor, Department of Computer Engineering, Hannam University, Daejeon 34430, Korea

[요 약]

최근 코로나바이러스 감염증으로 인해 도입이 빠르게 증가하고 있는 디지털 사이니지는 크게 3세대로 구분할 수 있다. 단순하게 정보를 제공하는 1세대 디지털 사이니지, 네트워크로 연결되어 디스플레이를 실시간으로 컨트롤 하는 2세대 디지털 사이니지, 상황인지 기술이 적용되어있는 3세대 디지털 사이니지로 구분 할 수 있으며 2세대, 3세대 디지털 사이니지의 경우 고객과 상호작용하기 위해 시스템, 디스플레이, 운영체제 등이 복잡하고 다양하게 적용되어 있어 보안에 많은 어려움을 겪고 있다. 본 논문에서는 해커의 공격으로 디지털 사이니지 시스템에 저장된 콘텐츠의 변조를 통한 스마트폰 보안사고를 실험하여 디지털 사이니지 콘텐츠의 보안 필요성에 대해 연구하였다.

[Abstract]

Digital signage, rapidly increased due to Covid-19, can be divided into three generations: the first generation that simply provides information, the second generation that controls the display in real time, connected to a network, and the third generation that applied situational awareness technology. There are many issues about security of the 2nd and 3rd generation digital signage as the systems, displays, and operating systems are applied in complex and diverse way in order to interact with customers. To shows the necessity for security of digital signage contents, this study conducts smartphone security experiments in which a cyber attack tampers with the contents stored in digital signage systems.

색인어 : 애플리케이션, 콘텐츠 보안, 디지털 사이니지, 악성코드, 스마트폰

Key word : Application, Contents Security, Digital Signage, Malware, Smartphone

http://dx.doi.org/10.9728/dcs.2021.22.7.1135

Received 25 June 2021; **Revised** 20 July 2021
Accepted 20 July 2021

***Corresponding Author; Woo-Young Soh**

Tel: +82-42-629-7657
E-mail: leejaeung1990@gamil.com

Ⅰ. 서 론

영화 마이너리티 리포트에 등장하는 디지털 디스플레이 광고판은 생체인식을 통해 맞춤형 광고가 노출된다. 마이너리티 리포트의 생체인식을 통한 디지털 디스플레이 광고판은 30대 남성이 지나갈 때 광고판은 고객이 좋아하는 맥주 광고, 자동차 광고를 내보낸다.

마이너리티 리포트에 등장하는 디지털 디스플레이 광고판을 지향하는 기술인 디지털 사이니지는 고객 맞춤형 광고를 제공하여 관심을 유도하기 때문에 광고효과를 극대화 할 수 있는 장점을 가지고 있다[1].

최근 코로나바이러스 감염증으로 인해 도입이 빠르게 증가하고 있는 디지털 사이니지는 크게 3세대로 구분할 수 있다. 단순하게 정보를 제공하는 1세대 디지털 사이니지, 네트워크로 연결되어 디스플레이를 실시간으로 컨트롤 하는 2세대 디지털 사이니지, 상황인지 기술이 적용되어있는 3세대 디지털 사이니지로 구분 할 수 있으며 2세대, 3세대 디지털 사이니지의 경우 고객과 상호작용하기 위해 시스템, 디스플레이, 운영체제 등이 복잡하고 다양하게 적용되어 있어 보안에 많은 어려움을 겪고 있다[2].

만약 해커의 공격으로 디지털 사이니지 콘텐츠의 변조가 발생하게 되면 고객이 디지털 사이니지와 양방향 소통을 하기 위해 사용하는 스마트폰의 보안사고가 발생할 수 있다.

본 논문에서는 해커의 공격으로 디지털 사이니지 콘텐츠의 변조를 통한 스마트폰 보안사고를 실험하여 디지털 사이니지 콘텐츠의 보안 필요성에 대해 연구하였다.

Ⅱ. 디지털 사이니지

2-1 개요

디지털 사이니지는 간판, 포스터 등과 같은 아날로그 광고판을 디지털 디스플레이를 활용하여 정보를 제공하는 디지털 광고판으로 정보의 전달력이 우수한 장점을 가지고 있다[3]. 과거에는 단순하게 정보만 제공하는 디스플레이의 역할을 했지만 와이파이, 블루투스, 비콘, 생체인식 등과 같은 IT기술과 융합하여 개인 맞춤형 서비스를 제공하고 있다[4][5].

개인 맞춤형 서비스를 제공하는 대표적인 디지털 사이니지로 코카콜라의 U-벤딩과, NTT도모코의 펨토셀이 있다. 코카콜라의 U-벤딩은 자판기의 디스플레이를 통해 광고를 보여주고, 블루투스를 이용하여 스마트폰으로 콘텐츠를 전송하며, NTT도모코의 펨토셀은 기지국 근처의 스마트폰 사용자를 파악하여 개인 맞춤형 광고를 디지털 사이니지로 제공하고 있다.

2-2 분류

디지털 사이니지는 단순하게 정보를 제공하는 일방적인 정보 제공 디지털 사이니지에서 세대가 바뀌어 갈수록 개인 맞춤형 서비스를 제공하는 디지털 사이니지로 변화하고 있으며 맞춤형 서비스의 형태에 따라 세대를 분류 할 수 있다.

1) 1세대 일방적인 정보 제공 디지털 사이니지

1세대 일방적인 정보 제공 디지털 사이니지는 아날로그 광고판을 디지털 디스플레이를 활용하여 콘텐츠를 통해 일방적으로 정보를 제공하는 형태를 가지고 있으며 대표적인 1세대 디지털 사이니지로 미디어 파사트가 있다[6]. 미디어 파사트는 디지털 디스플레이 대신 건물 외벽을 활용하여 디지털 사이니지를 구성하는 것이다. 서울 압구정동의 갤러리아 백화점 외벽에 구성한 미디어 파사트는 우리나라 최초의 미디어 파사트로 연간 약 1,200 만원의 유지비로 100억원 이상의 광고 효과를 보이고 있으며 광복 70주년을 기념하여 서울 스퀘어 외벽에 구성한 미디어 파사트는 태극기와 텍스트를 혼합한 콘텐츠를 제작하여 사람들의 많은 관심을 받았다.

2) 2세대 양방향 디지털 사이니지

2세대 양방향 디지털 사이니지는 일방적인 정보 제공이 아닌 고객 맞춤형 서비스를 제공한다는 점이 1세대 일방적인 정보 제공 디지털 사이니지와 차별성을 가진다. 기본적으로 네트워크에 연결되어 있어 디스플레이를 실시간으로 컨트롤 할 수 있으며, 고객과 양방향 커뮤니케이션을 통해 고객 맞춤형 서비스를 제공할 수 있는 장점을 가지고 있다[7]. 유동인구가 많은곳에 설치되어 고객 맞춤형 서비스를 실시간으로 제공하는 형태로 이용되고 있다. 대표적인 2세대 양방향 디지털 사이니지로 음식점, 쇼핑몰, 영화관에 설치되어 있는 터치스크린에 디지털 사이니지를 구성한 키오스크가 있으며 최근 코로나바이러스 감염증으로 인해 비대면 홍보, 주문이 가능한 키오스크의 수요가 증가하고 있다. 음식점에 설치되어 있는 키오스크는 고객에게 메뉴를 제공하고 고객은 음식과 음료, 결재 방식 등을 터치하여 주문할 수 있다. 또한 버스 정류장에 설치되어 있는 키오스크는 버스 배차시간과 버스 노선, 환승 정보 등을 제공하고 있다[8].

그림 1. 디지털 사이니지를 활용한 메뉴판
Fig. 1. Menu board using digital signage

그림 2. 코카콜라의 U-벤딩
Fig. 2. Coca-Cola's U-Vending

3) 3세대 상황인지 디지털 사이니지

3세대 상황인지 디지털 사이니지는 2세대 양방향 디지털 사이니지에 상황인지 기술, 인터페이스 기술을 등을 활용하여 더욱 적극적인 양방향 커뮤케이션이 가능하며, 실시간으로 고객 맞춤형 서비스를 제공할 수 있는 장점을 가지고 있다[8][10]. 대표적인 3세대 상황인지 디지털 사이니지로 엑스박스 키넥트, 닌텐도 위, 스마트폰을 이용한 디지털 사이니지 등 이 있다. 비디오 게임기에 일반적으로 사용되는 컨트롤러 대신 고객의 신체가 컨트롤러로서 제스처, 음성, 소리 등을 활용하거나, 스마트폰의 카메라, GPS, 블루트스, 비콘 등을 활용하여 3세대 상황인지 디지털 사이니지는 개인 맞춤형 서비스를 제공한다.

그림 3. 1세대 일방적인 정보 제공 디지털 사이니지(미디어 파사트)
Fig. 3. 1st generation unilateral digital signage (Media Passat)

그림 4. 2세대 양방향 디지털 사이니지(키오스크)
Fig. 4. 2nd generation interactive digital signage (Kiosk)

그림 5. 3세대 상황인지 디지털 사이니지(엑스박스 키넥트)
Fig. 5. 3rd generation situation-aware digital signage (Xbox Kinect)

Ⅲ. 디지털 사이니지 콘텐츠의 변조를 통한 스마트폰 보안사고 실험

3-1 악성코드 애플리케이션 제작

3세대 상황인지 디지털 사이니지는 개인 맞춤형 서비스를 제공하기 위해 스마트폰을 사용하여 고객과 상호작용한다. 고객에게 정보를 제공하기 위한 디지털 사이니지 콘텐츠에 해커의 공격이 발생하여 정상적인 콘텐츠가 아닌 악성코드가 유포되면 고객의 스마트폰에 저장되어 있는 민감정보의 탈취, 스마트폰의 카메라, GPS 등과 같은 기능을 제어하여 범죄에 악용될 수 있다.

정상적인 디지털 사이니지 콘텐츠가 아닌 악성코드 애플리케이션의 유포로 인한 스마트폰 보안사고 실험을 위해 악성코드 애플리케이션을 Kali Linux 64bit Version 운영체제에서 Metasploit 도구를 이용해 제작하였다.

1) LHOST 확인

악성코드 애플리케이션을 제작하기 전 악성코드와 연결할 PC의 LHOST가 필요하다. Kali Linux 64bit Version운영체제의 ifconfig 명령어를 이용하여 LHOST를 확인하였다.

2) 악성코드 애플리케이션 제작

Metasploit 도구를 이용하여 악성코드 애플리케이션을 제작하면 스마트폰의 민감정보를 탈취하고 카메라, GPS 등과 같은 스마트폰의 기능을 제어 할 수 있다. 악성코드 애플리케이션을 제작하기위해 Metasploit 도구의 msfvenom 명령어를 사용하였으며 malicious.apk 악성코드 애플리케이션을 제작하였다. 전 단계에서 확인한 LHOST를 악성코드 애플리케이션 제작에 사용하여 악성코드와 PC를 연결 할 수 있게 하였다.

3) signapk를 이용한 디지털 서명

안드로이드 운영체제의 애플리케이션은 디지털 서명이 요구된다. 디지털 서명이 되어있지 않은 애플리케이션 파일은 설

치할 수 없으며 디지털 서명은 애플리케이션의 개발자 인증에 사용된다. signapk는 디지털 서명이 되어있지 않은 애플리케이션에 디지털 서명을 하는 도구이다. 제작한 악성코드 애플리케이션 malicious.apk에 signapk를 이용하여 디지털 서명을 진행하였으며 디지털 서명이 완료된 악성코드 애플리케이션 signmalicious.apk을 제작하였다.

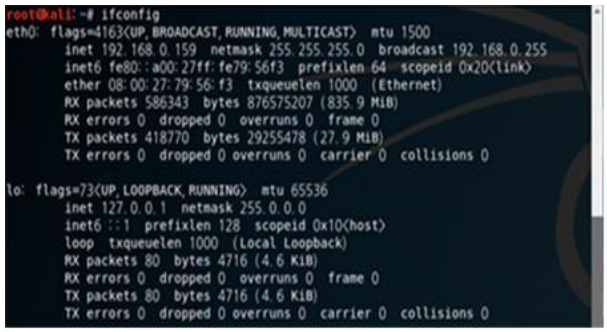

그림 6. ifconfig 명령어를 이용하여 확인한 LHOST
Fig. 6. LHOST verified using the ifconfig command

그림 7. Metasploit 도구를 이용해 악성코드 애플리케이션 제작
Fig. 7. Created a malware application using the Metasploit

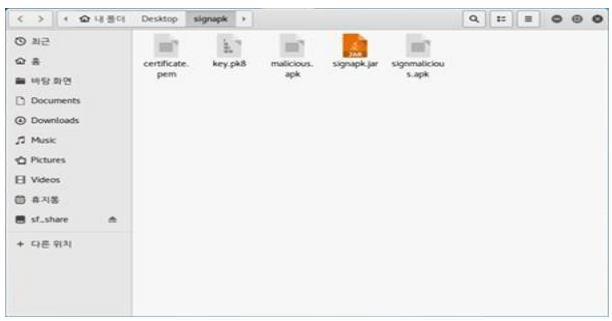

그림 8. signapk 도구를 이용해 디지털 서명한 악성코드 애플리케이션
Fig. 8. A malware application digitally signed using the signapk

3-2 정상적인 디지털 사이니지 콘텐츠 애플리케이션 변조

정상적인 디지털 사이니지 콘텐츠가 아닌 변조된 애플리케이션의 유포로 인한 스마트폰 보안 사고 실험을 위해 정상적인 디지털 사이니지 콘텐츠 애플리케이션을 Kali Linux 64bit Version 운영체제에서 TheFatRat 도구를 이용해 변조하였다.

1) LHOST 확인

정상적인 디지털 사이니지 콘텐츠 애플리케이션을 변조하기전 변조된 애플리케이션과 연결할 PC의 LHOST가 필요하다. Kali Linux 64bit Version운영체제의 ifconfig 명령어를 이용하여 LHOST를 확인하였다.

2) 정상적인 디지털 사이니지 콘텐츠 애플리케이션 변조

정상적인 디지털 사이니지 콘텐츠 애플리케이션을 악성코드가 포함된 애플리케이션으로 변조하기위해 TheFatRat 도구를 사용하였다. TheFatRat 도구의 다양한 기능 중 스마트폰의 민감정보를 탈취하고 카메라, GPS 등과 같은 스마트폰의 기능을 제거하기 위해 Backdooring Original apk를 사용하였으며 정상적인 디지털 사이니지 콘텐츠 애플리케이션을 변조하였다. 전 단계에서 확인한 LHOST를 애플리케이션 변조에 사용하여 변조된 애플리케이션과 PC를 연결할 수 있게 하였으며 정상적인 애플리케이션과 동일하게 작동하지만 악성코드가 포함되어 있는 변조된 애플리케이션을 제작하였다.

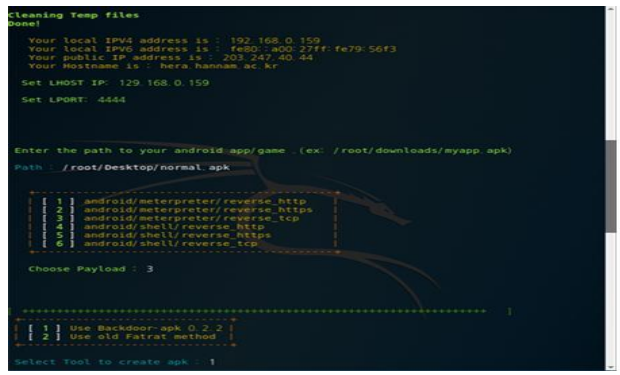

그림 9. 정상적인 디지털 사이니지 콘텐츠 애플리케이션 변조를 위해 사용한 TheFatRat 도구
Fig. 9. TheFatRat used to tamper with normal content of the digital signage application

3-3 테스트 배드 구성

해커가 디지털 사이니지를 공격하여 정상적인 디지털 사이니지 콘텐츠 대신 제작한 악성코드 애플리케이션과 변조된 악성코드 애플리케이션을 유포하는 상황을 가정한다. 디지털 사이니지 콘텐츠의 변조를 통한 스마트폰 보안사고 실험을 하기 위해 디지털 사이니지 콘텐츠 출력용 PC, 애플리케이션을 통해 스마트폰의 민감정보를 탈취하고, 스마트폰의 기능을 제어하는 제어용 PC, 디지털 사이니지와 상호작용하기 위한 스마트폰 3대를 사용해 테스트 배드를 구성하였다.

표 1. 디지털 사이니지 콘텐츠 출력용 PC
Table 1. PC for digital signage content output

CPU	Intel Core I7 920
RAM	12GB
OS	Windows 10 Pro 64bit
Digital Display	AOC 2769m

표 2. 스마트폰의 민감정보를 탈취하고, 스마트폰의 기능을 제어하는 제어용 PC
Table 2. PC for control that steals the sensitive information and controls the functions of the smartphone

CPU	Intel Core I7 3930K
RAM	16GB
OS	Kali Linux 64bit Version
Program	Metasploit Framwork Version(4.16.7-dev) Console Version(4.16.7-dev)

표 3. 디지털 사이니지와 상호작용하기 위한 스마트폰
Table 3. Smartphone to interact with digital signage

	Galaxy Note FE	Galaxy S8+	Galaxy Note 10
AP	Exynos 8	Exynos 9	Exynos 9
RAM	4GB	6GB	12GB
OS	Android 6	Android 8	Android 10

표 4. 추가실험에 사용한 스마트폰
Table 4. Smartphone used for additional experiments

	Galaxy S	Galaxy Note 10.1
AP	Exynos 3	Exynos 4
RAM	512MB	2GB
OS	Android 2.1	Android 4.1

3-4 악성코드 애플리케이션 유포로 인한 스마트폰 보안사고 실험

디지털 사이니지 콘텐츠 출력용 PC에 악성코드 애플리케이션을 유포하는 콘텐츠를 출력한다.

스마트폰 보안사고 실험 대상인 갤럭시 노트FE, 갤럭시 S8+, 갤럭시 노트10은 디지털 사이니지와 상호작용하기위해 디지털 사이니지 콘텐츠에 포함되어 있는 QR코드를 스캔하여 애플리케이션을 다운로드 하였다.

악성코드 애플리케이션 유포로 인한 스마트폰 보안사고 실험을 위해 다운로드 받은 악성코드 애플리케이션을 설치하였으나 실험대상은 비교적 최신 운영체제가 설치되어있어 악성코드가 포함되어있는 애플리케이션의 설치를 차단하였다.

그림 10. 디지털 사이니지를 통해 악성코드 애플리케이션을 유포하기 위한 QR코드
Fig. 10. QR code for distributing malware applications through digital signage

추가실험으로 안드로이드2.1, 안드로이드 4.1 운영체제를 가진 스마트폰에서 추가 실험을 진행했을 때 정상적으로 설치됨을 확인할 수 있었다.

악성코드 애플리케이션이 정상적으로 설치된 안드로이드 2.1, 안드로이드 4.1 기반의 스마트폰은 제어용PC에서 dump_contacts 명령과 webcam_snap 명령을 통해 저장되어있는 연락처를 탈취할 수 있었으며, 스마트폰의 카메라 기능 등을 제어할 수 있었다.

그림 11. 악성코드 애플리케이션 설치가 차단된 실험대상
Fig. 11. A test subject that blocks malware application installation

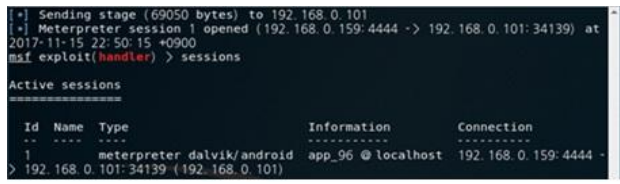

그림 12. 악성코드 애플리케이션이 설치되어 제어용 PC와 연결된 추가 실험대상
Fig. 12. Additional test subject connected to the PC for control with the malware application installed

3-5 변조된 애플리케이션 유포로 인한 스마트폰 보안사고 실험

디지털 사이니지 콘텐츠 출력용 PC에 변조된 애플리케이션을 유포하는 콘텐츠를 출력한다.

스마트폰 보안사고 실험대상인 갤럭시 노트FE, 갤럭시 S8+, 갤럭시 노트10은 디지털 사이니지와 상호작용 하기 위해 디지털 사이니지 콘텐츠에 포함되어 있는 QR코드를 스캔하여 애플리케이션을 다운로드 하였다.

변조된 애플리케이션 유포로 인한 스마트폰 보안사고 실험을 위해 다운로드 받은 변조된 애플리케이션을 설치하였고 정상적으로 설치됨을 확인할 수 있었다.

비교 실험을 위해 정상적인 애플리케이션과 변조된 애플리케이션을 설치했으며 실행결과 정상적인 애플리케이션과 변조된 애플리케이션 모두 정상적으로 작동함을 확인할 수 있었다. 하지만 정상적인 애플리케이션에 악성코드를 추가하여 변조하였기 때문에 변조된 애플리케이션을 실행하였을 때 실험대상

이 제어용 PC에 연결되었다.

제어용 PC에서 dump_sms 명령어를 이용하여 스마트폰의 민감정보인 문자메시지와 geolocate 명령어를 이용하여 스마트폰의 위치 좌표를 파악할 수 있었다.

그림 13. 디지털 사이니지를 통해 변조된 애플리케이션을 유포하기 위한 QR코드

Fig. 13. QR code for distributing tampered applications through digital signage

그림 14. 정상적인 애플리케이션(좌), 변조된 애플리케이션(우) 비교

Fig. 14. Comparison of normal application(left) and modulated application(right)

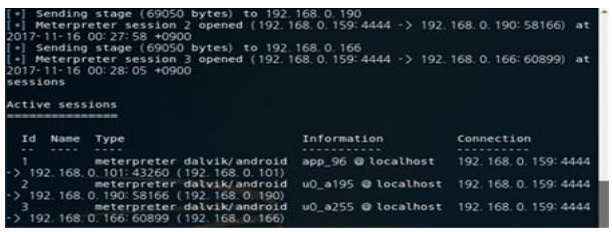

그림 15. 변조된 애플리케이션이 설치되어 제어용 PC와 연결된 실험대상

Fig. 15. A modulated application-installed test subject connected to the PC for control

그림 16. 제어용 PC에서 geolocate 명령어를 이용하여 파악한 스마트폰의 위치 좌표

Fig. 16. The location coordinate of the smartphone identified using the geolocate command on the PC for control

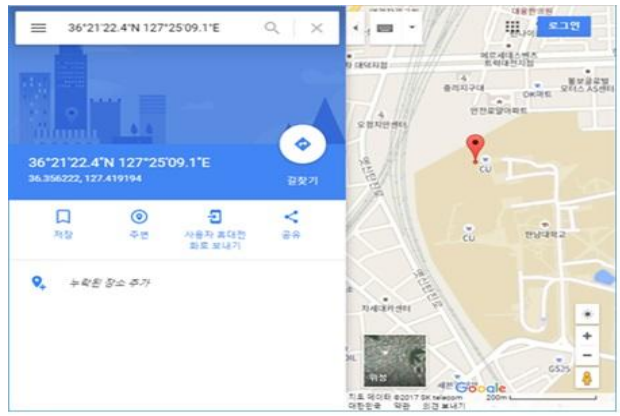

그림 17. Google Maps로 검색한 스마트폰의 위치 좌표

Fig. 17. The location coordinate of the smartphone searched by Google Maps

Ⅳ. 결 론

코로나바이러스 감염증으로 비대면 홍보 및 주문이 가능할 뿐만 아니라 고객 맞춤형 서비스를 제공하여 많은 사람들의 관심을 가지는 디지털 사이니지의 상용화가 빠르게 진행되고 있다. 그 중에서도 고객과 상호작용이 가능한 2세대 양방향 디지털 사이니지와 상황인지 기술이 적용된 3세대 상황인지 디지털 사이니지의 요구가 증가되고 있으며 디지털 사이니지와 고객이 상호작용 하기위해 고객의 스마트폰을 사용하는 디지털 사이니지의 개발이 계속되고 있다.

하지만 2세대 양방향 디지털 사이니지와 3세대 상황인지 디지털 사이니지를 구성하기 위해 시스템, 디스플레이, 운영체제 등이 매우 복잡하고 다양하게 적용되어 있어 보안에 많은 어려움을 겪고 있다.

본 논문에서 진행한 디지털 사이니지 콘텐츠의 변조를 통한 스마트폰 보안사고 실험결과 스마트폰에 저장되어있는 민감정보 탈취 뿐만 아니라 스마트폰의 카메라, GPS등과 같은 기능을 제어할 수 있었다.

디지털 사이니지 콘텐츠의 변조를 통해 탈취한 민감정보와 스마트폰의 카메라, GPS 등과 같은 기능제어를 통해 범죄의 대상이 될 수 있기 때문에 디지털 사이니지 콘텐츠 보안이 요구된다.

또한 후속 연구로 디지털 사이니지 콘텐츠의 보안을 위해 인공지능 악성코드 탐지가 가능한 디지털 사이니지 콘텐츠 서버를 설계하고 구현하여 해커의 공격으로부터 디지털 사이니지 콘텐츠를 보호하는 후속연구를 진행하고자 한다.

감사의 글

이 논문은 2019년도 한남대학교 학술연구비 지원에 의하여 연구되었음.

참고문헌

[1] K. H. Ro, “A Research on Context-aware Digital Signage using a Kinect,” *The journal of the Institute of Internet Broadcasting and Communication*, Vol. 14, No. 1, pp. 265-273, Feb 2014.

[2] J. U. Lee, R. Y. Jang, S. J. Jung, K. Sung, W. Y. Soh, “A Study on the Necessities of Content Security for a Digital Signage System,” in *Proceedings of KIIT Conference*, Daejeon, pp. 68-72, 2017.

[3] H. N. Lee, “A Study on a Plan of Digital Signage Activation as an Advertising Medium,” *Journal of The Korean Society Design Culture*, Vol. 17, No. 2, pp. 502-517, Jun 2011.

[4] J. U. Lee, A Design for a Secured Digital Signage System with Content Servers, MS. dissertation, Hannam University, Daejeon, 2018.

[5] H. S. Ahn, “Research on Strategy of User Experience-Oriented Interactive Digital Signage,” *The Korea Society of Art & Design*, Vol. 23, No. 1, pp. 251-265, Mar 2020.

[6] C. O. Yun, “Development of Smart Contents Platform for providing Digital Sinage Environment,” *Journal of the Korea industrial information systems society*, Vol. 20, No. 2, pp. 25-37, Apr 2015.

[7] K. H. Ro, “A Research on Personalized Mobile Advertising Service using the Linkage between Digital Signage and Smartphones,” *The journal of the Institute of Internet Broadcasting and Communication*, Vol. 14, No. 1, pp. 139-146, Feb 2014.

[8] S. W. Shim, “The Study on Application of QR code to Digital Signage,” *The Korean Journal of Advertising*, Vol. 23, No. 5, pp. 187-214, Jul 2012.

[9] S. H. Cha, “A Study on the Status and Implication of Digital signage in Korea - For Design field,” *Korea Digital Design Council*, Vol. 16, No. 3, pp. 115-126, Sep 2016.

[10] E. S. Nahm, “Development of Multi-Touch/Context-Aware Convergence Digital Signage System based on Android OS Platform,” *Journal of Digital Convergence*, Vol. 13, No. 8, pp. 245-251, Aug 2015.

이재웅(Jae-Ung Lee)

2018년 : 한남대학교 대학원 (공학석사)
2018년～현 재 : 한남대학교 대학원 (박사과정)

2018년～현 재: 한남대학교 탈메이지교양교육대학 강사
2021년～현 재: 목원대학교 융학컴퓨터미디어학부 강사
2021년～현 재: 우송대학교 우송교양대학 초빙교수
※관심분야 : 정보보안, 시스템보안, 디지털포렌식, 디지털사이니지, 머신러닝 등

소우영(Woo-Young Soh)

1981년 : 서울대학교 대학원 (이학석사)
1990년 : 메릴랜드대학교 대학원 (이학박사-소프트웨어인공지능)

1991년～현 재: 한남대학교 컴퓨터공학과 교수
※관심분야 : 클라우드컴퓨팅, 정보보안, 사물인터넷, 디지털사이니지, 머신러닝 등