

2019 한국정보보호학회 하계학술대회

# CISC-S'19

Conference on Information Security and Cryptography-Summer 2019

2019. 6. 20(목)~22(토)

부산 동명대학교 (제1정보통신관, 중앙도서관)

주최



**한국정보보호학회**  
Korea Institute of Information Security & Cryptology

주관



**동명대학교**  
TONGMYONG UNIVERSITY

후원



**국가정보원**  
National Intelligence Service Korea



**과학기술정보통신부**



**행정안전부**



**KISA 한국인터넷진흥원**

**ETRI**

**한국전자통신연구원**  
Electronic and Telecommunications  
Research Institute

**NSR**

**국가보안기술연구소**  
National Security Technology Research Institute

**IITP**

**정보통신기획평가원**

**AhnLab**

## TRACK 1 - 313호 소강의실

| 세션                                           | 발표논문                                                                               |
|----------------------------------------------|------------------------------------------------------------------------------------|
| <b>A1</b><br><b>해킹1</b><br>좌장 : 김호원 교수 (부산대) | Selenium과 실시간 이벤트 로그 기반 악성 웹사이트 탐지 시스템 제안<br>김민재, 엄홍열 (순천향대학교)                     |
|                                              | 한글 파일에 글자색과 글자크기 조작을 통해 은닉된 데이터의 탐지 기법에 대한 연구<br>변상필 (대구가톨릭대학교)                    |
|                                              | TF-IDF 기반 PE파일 Embedding 기법을 통한 악성코드 유형분류 기술 연구<br>하지희, 이태진 (호서대학교)                |
|                                              | DNN 기반 Packer 유형 분류기술 연구<br>이영주, 이태진 (호서대학교)                                       |
|                                              | DLL Ejection 방식을 통한 DLL Injection 공격 탐지 및 대응<br>장준영, 이종윤, 임을규 (한양대학교)              |
| <b>B1</b><br><b>해킹2</b><br>좌장 : 김경곤 교수 (고려대) | kNN 기반 악성코드 분석 최적화 방안 연구<br>황찬웅, 이태진 (호서대학교)                                       |
|                                              | ICS 환경에서의 Air-gap 공격 분석<br>고영민, 고주성, 광진 (아주대학교)                                    |
|                                              | 힙 익스플로잇 탐지를 위한 프리미티브 설계<br>채수민, 진홍주, 이동훈 (고려대학교)                                   |
|                                              | 안드로이드 악성코드 탐지를 위한 자연어 처리 기반의 API 특징 추출 기법<br>이동재, 윤재현, 오원휘, 차오녹투, 정수환 (숭실대학교)      |
|                                              | 안드로이드 CFG와 API 그룹화를 이용한 악성코드 분류 기법에 대한 연구<br>심현석, 박정수, 천호진, 단티엔복, 정수환 (숭실대학교)      |
| <b>C1</b><br><b>해킹3</b><br>좌장 : 이재철 교수 (호서대) | 지능형 안드로이드 악성코드 유형 분석 및 대응 방안<br>윤홍선, 오원부령, 조하은, 정수환 (숭실대학교)                        |
|                                              | 음악 스트리밍 서비스의 콘텐츠 다운로드 취약성 분석<br>장한빈, 김형식 (성균관대학교)                                  |
|                                              | 블루 필터를 이용한 SSD-Insider 알고리즘에 대한 성능 향상<br>김정현*, 정창훈*, 양대현*, 이경희** (*인하대학교, **수원대학교) |
|                                              | Spectre의 취약점 및 변종 공격 동향 연구<br>한찬희, 이만희 (한남대학교)                                     |
|                                              | 모바일 어플리케이션 개인정보 유출 취약성 분석<br>지우중, 김형식 (성균관대학교)                                     |

## ICS 환경에서의 Air-gap 공격 분석

고영민\*, 고주성\*\*, 콰진\*\*\*

\*,\*\*\*아주대학교 사이버보안학과

\*\*아주대학교 컴퓨터공학과, 정보보호응용및보증연구소

### Air-gap Attack Analysis on ICS Environment

Young-min Ko\*, Ju-Seong Ko\*\*, Jin Kwak\*\*\*

\*,\*\*\*Department of Cyber Security, Ajou University.

\*\*ISAA Lab., Department of Computer Engineering, Ajou University.

#### 요 약

IT 기술의 발전에 따라 산업 제어 시스템(ICS)에 해당하는 원자력 발전소나 자동화 생산시설과 같은 사회기반시설들은 대부분 망 분리를 통해 시설을 보호하고 있다. 이러한 사회기반시설에 해당하는 인프라는 전력, 수도 등 높은 가치의 자원을 지니고 있고, 침해사고 발생 시 비가역적인 손실이 발생할 수 있다. 또한, ICS는 산업 규모의 증가로 제어의 효율성을 증가시키기 위해 네트워크 기반의 연결을 늘리고 있으며, 이에 따라 공격 빈도와 피해 심각성이 증가하고 있으나, ICS와 같은 국가기반시설의 보안은 망 분리에 의존하고 있는 실정이다. 따라서 본 논문에서는 망 분리 환경에 대한 Air-gap 공격에 대하여 분석하고, 이에 대한 대응방안을 제시한다.

#### I. 서론

미국의 홈랜드 시큐리티 산하기관 ICS-CERT의 자료를 분석한 Positive Technologies사의 연간보고서에 따르면, ICS에 대한 공격의 빈도와 침해사고의 심각성은 지속해서 증가하고 있다[1]. 일례로 2015년 Black energy에서 2016년 Industroyer를 거쳐 2017년 TRITON에 이르기까지 ICS를 대상으로 하는 멀웨어들은 지속해서 활동하고 있다.

이러한 ICS에의 보안 요소로 가장 먼저 고려되며 큰 비중을 차지하는 것이 망 분리지만, ICS상에는 이미 다양한 종류의 공격 시도가 있었고 성공사례가 존재하는 만큼 망 분리는 절대적인 보안 장치가 될 수 없다. 따라서 본 논문에서는 멀웨어가 어떻게 망

분리 환경을 통과하여 공격을 성공시킬 수 있는지 그 과정에 대하여 분석하고자 한다.

본 논문의 구성은 다음과 같다. 2장에서는 Air-gap의 정의와 ICS 환경에서 상정 가능한 대표적인 Air-gap 은닉 채널에 대해 설명한다. 3장에서는 망 분리 환경에 대한 Air-gap 멀웨어 들의 침투 방식을 분석하고 이러한 공격들에 대한 대응방안을 제시한다. 이후 마지막으로 4장에서 결론을 맺는다.

#### II. 관련연구

##### 2.1 Air-gap

Air-gap이란 물리적으로 두 네트워크를 단절하고, 두 네트워크 간의 정보 및 자원의 공유를 최소화함으로써 외부의 개입을 가능한 줄이는 방식이다. ICS와 같은 중요 시설에는 Air-gap을 통한 보안 기법이 적용된 경우가 많다. 따라서 ICS에 대한 공격이 이루어지기 위해서는 Air-gap을 우회하는 것이 필요하다.

---

이 논문은 2019년도 정부(과학기술정보통신부)의 재원으로 한국연구재단의 지원을 받아 수행된 연구임(No. NRF-2017R1E1A1A01075110).

## 2.2 Air-gap 은닉 채널

Air-gap을 적용하더라도 외부 네트워크와의 접점을 완전히 차단할 수 없다. 이처럼 의도하지 않게 외부 네트워크와 연결된 접점을 은닉 채널이라고 부르며, Air-gap을 우회하기 위한 은닉 채널들은 아래 [표 1]과 같다.

[표 1] Air-gap 상에서의 은닉 채널

| 분류              | Attack surface                          |
|-----------------|-----------------------------------------|
| Acoustic        | fan, Disk, Speaker                      |
| Optical         | CCTV, Drone                             |
| Electromagnetic | FM radio, TV, Bluetooth, CPU-memory bus |
| Magnetic        | Magnetic facility                       |
| Electric        | Electric Panel                          |
| Thermal         | CPU, GPU, HDD, Motherboard              |
| Physical Media  | USB flash drive                         |

## III. Air-gap 멀웨어 분석

2장에서 다룬 바와 같이 Air-gap에는 여러 은닉 채널이 존재한다. 이 장에서는 ICS상에서 Air-gap 우회에 주로 사용될 수 있는 은닉 채널과 이를 통한 망 분리 환경상에서의 공격 사례를 통해 멀웨어를 분석한다.

### 3.1 Physical Media

Physical Media 영역에서의 공격은 Stuxnet이 있다. Stuxnet은 공급망 공격을 통해 ICS 내부로 Air-gap을 통과한 사례로, 내부 제로데이 모듈을 제외하고도 USB를 통한 PLC 제조과정에서의 엔지니어 단말 감염을 주요 우회 기법으로 사용하였다[2]. 이러한 Stuxnet의 작동 메커니즘은 아래와 같다.

**Step 1.** LNK Zeroday를 이용한 PLC 탐색

**Step 2.** PLC 탐색 및 네트워크상에 연결된 단말 추가 탐색

**Step 3.** 사용자 도메인 인증 사용 및 CAS 서버로 웹 전파

**Step 4.** CAS DB 및 Stored Procedure 조작을 통한 웹 설치

**Step 5.** 공정 제어 네트워크 및 제어 시스템 네트워크로 전파 및 C&C 서버 연결

## 3.2 Electromagnetic

이 은닉 채널에서 Air-gap 우회에 성공한 대표적인 예로는 Blueborne 등이 있다. Blueborne은 블루투스 기능을 가진 단말들에 적용될 수 있는 공격으로, 이에 사용되는 취약점들을 표로 나타내면 아래 [표 2]와 같다[3].

[표 2] Blueborne 취약점

| 분류               | 설명                               |
|------------------|----------------------------------|
| CVE-2017-0781    | 안드로이드 테더링 과정에서 발생하는 원격 코드 실행 취약점 |
| CVE-2017-8628    | 윈도우의 블루투스 드라이버에서 발생하는 스푸핑 취약점    |
| CVE-2017-1000251 | 리눅스 커널 원격코드 실행 취약점               |
| ...              | ...                              |

Blueborne의 작동 메커니즘은 아래와 같다.

**Step 1.** Host의 블루투스 작동 여부 탐색

**Step 2.** 내재한 취약점을 통한 익스플로잇

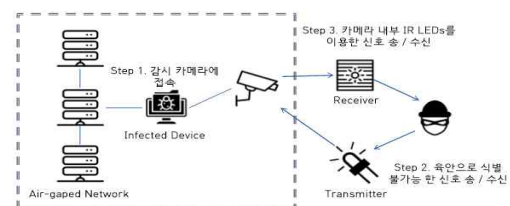
**Step 3.** 악성 행위 수행

**Step 4.** C&C 서버와의 지속적인 통신 수행

Bluetooth 외에도 Electromagnetic에서 상정 가능한 공격시나리오로는 2장에서 제시한 것처럼 FM 주파수, 블루투스 등의 단거리 무선 통신을 이용할 수 있고, 멀웨어들은 이러한 단거리 무선 통신용 주파수에서의 빈도나 진폭 등을 이용하여 Air-gap을 우회하는 수단으로 활용할 수 있다.

## 3.3 Optical

Optical 은닉 채널에서의 Air-gap 우회에 성공한 대표적인 사례로는 aIR-Jumper 등이 있다. aIR-Jumper의 작동 메커니즘을 그림으로 나타내면 아래 (그림 1)과 같다[4].



(그림 1) aIR-Jumper 작동 메커니즘

**Step 1.** 감염된 CCTV 제어 서버에 접속

**Step 2.** CCTV 감시구역 내에 육안으로는 인지되지 않는 LED indicator를 transmitter로 사용하여 점멸 신호를 전송

**Step 3.** CCTV 카메라 내부의 IR LED를 Receiver/Transmitter로 삼아 미리 설치한 Receiver를 향한 적외선 신호 전송을 통해 양방향 통신 수행

**Step 4.** C&C 서버 / 공격자와의 통신 지속

본 논문에서는 aIR-Jumper 사례만 분석하였으나, 일반적으로 Optical 은닉 채널에서의 상정 가능한 공격시나리오로는 CCTV의 LED indicator나 TV 화면 등을 이용해, 모니터링 중인 화면에 멀웨어로 하여금 인코딩된 점멸주기를 신호로 활용하여 송/수신함으로써 Air-gap을 우회할 수 있다.

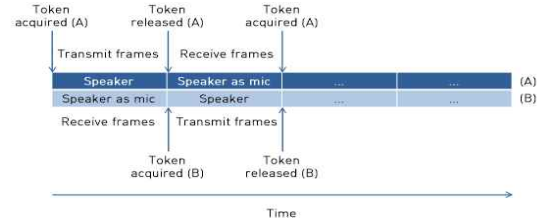
### 3.4 Acoustic

Acoustic 은닉 채널 영역에서의 Air-gap 우회에 성공한 대표적인 예시는 MOSQUITO 등이 있다. MOSQUITO는 일정 음역의 토큰을 지정하고, 이에 대한 송/수신자를 지정함으로써 양방향 통신을 수행한다. 또한, 이를 위해서 토큰에 대한 컨트롤 메시지를 프로토콜로써 정의하고 사용한다. MOSQUITO 컨트롤 메시지 프로토콜을 표로 나타내면 아래 [표 3]과 같다[5].

[표 3] MOSQUITO 컨트롤 메시지

| 메시지         | 설명                                |
|-------------|-----------------------------------|
| DISCOVERY   | The discovery broadcast message   |
| ACQUIRE     | Acquire the transmission token    |
| RELEASE     | Release the transmission token    |
| ACK_OK      | Frame received successfully (ack) |
| RETRANSMIT  | Request to retransmit a frame     |
| BITRATE_INC | Increase the current bit rate     |
| BITRATE_DEC | Decrease the current bit rate     |

이러한 MOSQUITO를 이용한 임의의 단말 A와 B의 통신 프로토콜을 그림으로 나타내면 아래 (그림 2)와 같다[5].



(그림 2) MOSQUITO Communication Protocol

아래는 MOSQUITO의 통신 메커니즘이다.

**Step 1.** 단말 A가 특정 음역 발신자 토큰을 수신하고, 발신자가 됨

**Step 2.** 단말 B가 수신자로서 정보를 수신함

**Step 3.** 단말 A가 특정 음역 발신자 토큰을 발신하고, 수신자가 됨

**Step 4.** 위 과정을 A, B 단말이 반복하여 양 단말 간 통신을 수행함

MOSQUITO의 경우 스피커라는 매체를 이용하여 Air-gap을 우회하였으나, Acoustic에서의 상정 가능한 공격시나리오로는 초음파 대역을 이용한 방법을 가정할 수 있다. 이에 이용되는 장치로는 스피커나 CPU/GPU 등의 팬 등이 있으며, 멀웨어는 오디오 칩의 취약점을 이용해 스피커로 통신 채널을 구축하여 입/출력을 교환함으로써 단말 간의 통신을 통해 Air-gap을 우회할 수 있다.

### 3.5 은닉 채널 기반 Air-gap 멀웨어 분석

본 논문에서는 ICS Air-gap 상에서의 은닉 채널 중 Physical Media, Electromagnetic, Optical, Acoustic의 Attack surface에서의 Air-gap 공격에 대하여 분석하였다. 이러한 각각의 영역에서의 은밀성, 채널 가용성, 감염 단말에서의 요구 권한 수준을 정리하여 표로 나타내면 아래 [표 4]와 같다.

[표 4] Air-gap Attack 분류 및 분석

| 분류     | Physical Media | Electromagnetic | Optical | Acoustic |
|--------|----------------|-----------------|---------|----------|
| 은밀성    | 낮음             | 높음              | 높음      | 높음       |
| 채널 가용성 | 높음             | 높음              | 낮음      | 높음       |
| 요구 권한  | 일반             | 일반 / 루트         | 일반      | 일반       |

[표 5] Air-gap Attack 대응방안

| 대응방안                                         | 대응영역     | 은닉 채널                                              |
|----------------------------------------------|----------|----------------------------------------------------|
| 단말 간의 구역 지정 및 물리적 격리, Red-Black Architecture | 물리 영역    | Physical Media, Acoustic, Electromagnetic, Optical |
| 케이블 또는 패널 등의 내/외부 차폐                         | 하드웨어 영역  | Electromagnetic                                    |
| Signal filtering                             | 하드웨어 영역  | Electromagnetic, Acoustic                          |
| Signal jamming                               | 하드웨어 영역  | Electromagnetic                                    |
| 행위 분석<br>/ User Behavior Analysis            | 소프트웨어 영역 | Physical Media, Acoustic, Electromagnetic, Optical |
| 단말 전자기장 방출 제어 기법<br>(Soft Tempest)           | 소프트웨어 영역 | Electromagnetic                                    |

#### IV. 결론

[표 4]에서의 Air-gap 멀웨어들에 대한 분석을 토대로 대응방안을 해당 영역과 은닉 채널에 따라 분류하여 제시하면 [표 5]와 같다.

본 논문에서는 Air-gap으로 분리되는 ICS와 같은 환경에서의 공격을 주요 목표로 하는 멀웨어들에 대해 분석하였으며, 해당 멀웨어들이 이용하는 은밀 채널과 침투 방식에 대한 대응방안을 제시하였다. 제안하는 대응방안으로는 물리 / 하드웨어 / 소프트웨어 측면에서의 대응방안들을 제시하였다.

따라서 본 논문을 통해 ICS와 같은 망 분리 환경에서의 Air-gap 안전성을 보다 증가시킬 수 있다. 그러나 각각의 대응방안은 단순한 Mitigation에 대응하는 방안이며, 기술의 발전과 IoT 등 새로운 기술의 도입으로 인해 언제든 새로운 Attack Surface가 발생할 수 있다.

따라서 향후 연구 계획으로는 제안한 대응방안 중 행위 분석 대응방안을 발전시켜, 최종적으로는 ICS 환경에서의 사용자 행위 분석을 통한 폐쇄망 내부 관제 시스템을 설계하고자 한다.

#### [참고문헌]

- [1] Positive Technologies, "ICS Security: 2017 in review", <https://www.ptsecurity.com/ww-en/analytics/ics-security-2017/>, Positive Technologies, pp. 4-13, Feb. 2018.
- [2] Karnouskos and Stamatis, "Stuxnet worm impact on industrial cyber-physical system security", IECON 2011-37th Annual Conference of the IEEE Industrial Electronics Society, IEEE, pp.2-4, Nov. 2011.
- [3] Seri, B. and Vishnepolsky, G., "Blueborne Technical White Paper", <https://go.armis.com/hubfs/BlueBorne%20Technical%20White%20Paper-1.pdf?t=1513642788073>, Armis, pp. 3, Dec. 2018.
- [4] Mordechai Guri, Dima Bykhovsky, "aIR-Jumper: Covert air-gap exfiltration/infiltration via security cameras & infrared (IR)", Computers & Security, Volume 82, pp. 15-29, Dec. 2018.
- [5] M. Guri, Y. Solewicz and Y. Elovici, "MO SQUITO: Covert Ultrasonic Transmissions Between Two Air-Gapped Computers Using Speaker-to-Speaker Communication," 2018 IEEE Conference on Dependable and Secure Computing (DSC), Kaohsiung, Taiwan, pp. 1-8, Dec. 2018.