수사 관점에서의 보이스피싱에 활용되는 CMC 기능 및 아티팩트 분석

유민정 [1], 박승현 [1], 김성민 [2]
[1] 성신여자대학교 융합보안공학과 학부생
[2] 성신여자대학교 융합보안공학과 교수

20211079@sungshin.ac.kr, 20211058@sungshin.ac.kr, sm.kim@sungshin.ac.kr

Analysis of CMC Call used in Voice Phishing & Artifact from the perspective of investigation

Min-Jung Yoo[1], Seung-hyun Park[1], Seong-Min Kim[1]
[1]Dept. of Convergence Security Engineering, Sungshin Women's University

요 약

삼성 스마트폰 계정 기반 서비스인 다른 기기에서 전화/문자하기(CMC) 기능이 보이스피싱의 새로운 기술로 동원되고 있다. 기존의 심박스와 같은 불법 중계기보다 발신 번호 변작에 쉽게 활용할 수 있어 CMC 기능을 악용한 보이스피싱 범죄가 증가하고 있으나, 이에 대한 연구가 미비한 현실이다. 본 논문에서는 삼성 기기에서의 CMC 활성화 및 기능 사용 여부에 따른 안드로이드 시스템 로그에서의 차이를 분석하고, 이를 바탕으로 보이스피싱 수사에 활용할 수 있는 포렌식 아티팩트 분석 방법을 제안한다.

1. 서론 및 배경 지식

보이스피싱은 최근까지도 심각한 사회 문제로 인식되고 있으며, 2023 년의 피해 금액은 전년 대비 514 억 원이 증가한 1,965 억 원으로 그 규모 또한 꾸준히 증가하고 있다 [1]. 과거 보이스피싱 범죄자들은 해외 또는 인터넷 번호를 국내 번호로 표시하기 위해 VoIP 게이트웨이 또는 심(SIM)박스 등의 불법 중계기를 사용하였으나, 최근에는 유심(USIM)과 함께 삼성 스마트폰, 태블릿 PC 에서 제공하는 다른 기기에서 전화/문자하기(Call&Message Continuity, CMC) 기능을 새로운 기술로 동원하고 있다.

CMC 는 스마트폰과 연동된 다른 단말에서 통화나 메시지를 발신할 수 있는 스마트폰 계정 기반 서비스로, 본래 사용자 편의를 위하여 제공되었다. 그러나 이를 악용하는 보이스피싱 범죄의 확산으로 인해 수사 관점에서 CMC 보이스피싱에 대한 디지털 증거 확보의 필요성이 커지고 있다. 따라서 본 논문에서는 안드로이드 시스템 로그 분석을 통해 디바이스의 CMC 활성화 및 기능 사용 여부를 탐지할 수 있는 포렌식 아티팩트 분석 방법을 제안하고자 한다.

1.1. CMC 를 이용한 보이스피싱

CMC 기능은 동일한 삼성 계정을 사용하는 태블릿 PC, 스마트워치 등으로 삼성 스마트폰의 통화와 메시지를 사용할 수 있도록 해주는 서비스이다. 안드로이드 9 이상인 삼성 기기에서 지원되며, 같은 네트워크가 아니더라도 인터넷이 연결된 환경에서 어디서든 사용할 수 있다. CMC 로 연결된 기기 간에는 해외에서 통화 발신을 하더라도, 국내 기기를 거쳐 국내 번호로 표시할 수 있다. 이를 악용할 경우, 기존 불법 중계기를 통한 보이스피싱 대비 사용이 간편하고 추적을 피하기 쉬워 보이스피싱 범죄에 악용되는 사례가 증가하고 있다. 최근 국내 삼성 스마트폰과 해외 기기 간의 CMC 를 이용하여 2 억 3,915 만원을 편취한 보이스피싱 조직이 검거되었으며[2], 피해금액이 빠르게 증가하고 있는 만큼 신속한 수사가 필요하다.

1.2. CMC 통화 분석 및 탐지

수사기관은 가능한 보이스피싱 조직원이 소유한 모든 기기를 확보하여 범죄 흐름을 파악해야 한다. 그러나 현재 CMC 를 이용한 보이스피싱에 대한 연구는 불법 중계기 탐지 연구 대비 미흡하여 제대로 확립된 수사 방법을 찾아보기 어렵다. 안준호 외 8 인은 SSRC ID 와 음성 RTP 패킷의 지연차를 이용한 CMC 통화 탐지 방법을 제안하였다[3]. 일반 통화와 달리 CMC 통화는 PD(Primary Device)와 Victim,

SD(Secondary Device)와 Victim 사이에 통화 세션이 각각 생성된다. 이로 인해 RTP 패킷의 지연이 발생하고 두 번째 세션이 생성될 때 SSRC ID, Seq 값이 다른 값으로 변경되는데, 이러한 특징을 통해 CMC 통화의 탐지가 가능함을 보였다. 그러나 해당 방법은 네트워크 트래픽 수집이 필요하며 기기 내 정보를 바탕으로 한 분석 방법으로 보기 어렵다는 한계점을 가진다.

2. Android Dumpstate Log 분석

안드로이드 Dumpstate Log 분석을 통해 유심이 장착되어 있는 PD 와 유심이 없는 SD 간의 CMC 활성화 여부 및 활성화 전후의 통화에서 나타나는 차이를 확인하였다. 이때, PD 로 LG U+ 유심을 장착한 Galaxy Flip 5 를, SD 로 Galaxy Tab S9 FE 를 사용하였다.

2.1. CMC 활성화

그림 1 은 CMC 를 활성화했을 때 SD 에서 나타나는 로그의 일부로, PD 와 SD 의 CMC 연결이 성공적으로 수행되었음을 식별할 수 있다. 유심이 장착된 일반적인 기기는 RCS 기능이 포함된 앱을 실행하거나 통화 및 문자 등을 할 때 RCS-ImsUI 에 관한 로그가 남는다. SD 에서는 CMC 를 활성화했을 때만 해당 로그가 생기며, 인스턴스의 식별자는 매번 달라진다.

```
ContactApplication[contacts](u0): ContactsApplication started!
…
RCS-ImsUiFactory[dialer](u0): create imsServiceCarrier : KOR
RCS-ImsUiFactory[dialer](u0): create imsServiceCarrier : KOR
RCS-ImsUiManagerFactory[dialer](u0): New instance created:rf.k@fe97cf2
```

(그림 1) CMC 활성화 시 SD 에 나타나는 로그.

반면 PD 의 경우, CMC 를 활성화하여도 유의미한 로그가 발견되지 않았다. 따라서 CMC 보이스피싱 활용 여부를 판단하기 위해서는 이용된 기기들 중 SD 에 해당하는 기기를 중점으로 분석하여야 한다.

2.2. CMC 통화

일반적인 통화에서 발신 기기의 로그와 CMC 를 이용한 통화에서의 PD, SD 로그를 비교 분석하였다.

```
TelephonyModel[dialer](u0): isRoamingLGT slotId : 0, isRoamingState :false
CallLogProvider[system](u0): insert : uri = content://logs/call?
RoamingScoreConcept[system](u0): context com.android.providers.contacts.sec.ContactsProvider …
RoamingScoreConcept[acore](u0): RAD formattedNumber : 010…
RoamingScoreConcept[system](u0): RAD update : last_score=90 last_duration=119 number=010…
```

(그림 2) 일반적인 통화에서 발신 기기에 나타나는 로그.

유심이 장착된 기기 간의 통화에서 발신 기기의 로그는 그림 2 와 같으며, 로밍 국가와 통화 유형, 연락처에 저장된 수신자의 전화번호 및 이름 등의 정보가 로그에 나타난다.

```
CallLogProvider[system](u0): insert : uri = content://logs/call?ROAMING_AUTO_DIALER=KR...
RoamingScoreConcept[system](u0): context
com.android.providers.contacts.sec.ContactsProviderApplication@d805a6f number : 010…
CallLogProvider[system](u0): Delete(1) calllog by limit. groupId(null), callLog_id(160, …
```

(그림 3) CMC 를 이용한 통화에서 PD 에 나타나는 로그.

```
TelephonyDataSource[dialer](u0): subscriptionInfos is null.
CallLogProvider[mdecservice](u0): insert : uri=content://log/call pid = 6669
CallLogProvider[mdecservice](u0): current max callLog count: 2000
```

(그림 4) CMC 를 이용한 통화에서 SD 에 나타나는 로그.

그림 3 는 CMC 로 이루어진 통화에서 PD 에 나타나는 로그의 일부이며, 그림 4 는 SD 에 나타나는 로그이다. PD 의 로그는 일반적인 통화와 유사했으나, RAD 설정에 관한 로그가 나타나지 않는 차이를 보인다. SD 의 로그에는 수신자 및 통화와 관련된 특징적인 정보가 드러나지 않는다.

<표 1> 일반 통화와 CMC 통화의 로그 비교

	일반 통화	PD	SD
로밍 국가	O	O	X
수신자 정보	O	O	X
RAD 설정	O	X	X

통화 로그에서의 대표적인 차이를 표 1 에 정리하였다. CMC 를 이용한 보이스피싱에서 통화에 대한 정보는 유심이 장착되어 있는 PD 측에 남으므로, PD 의 통화 로그 정보를 통해 신고되지 않은 보이스피싱 피해자를 사전에 발견할 수 있다.

3. 결론

본 논문에서는 CMC 를 활용한 보이스피싱 탐지 수사 관점에서 디지털 증거를 확보할 수 있는 방법을 제안한다. 안드로이드 시스템 로그를 통해, SD 에서 CMC 활성화 과정을 파악하고 PD 에서 통화 설정 및 수신자의 정보를 파악한다면 CMC 를 이용한 보이스피싱을 탐지할 수 있다. 향후 연구로는 SD 에서 PD 의 디바이스를 식별하고, PD 와 SD 의 기기를 다변화했을 때의 차이를 분석하는 연구를 진행할 예정이다.

참고문헌

[1] “Each victim of voice phishing lost 17 million won, up 1.5 times from the previous year”, accessed on Mar. 08, 2024, https://eiec.kdi.re.kr/policy/materialView.do?num=248897

[2] “Controlling the Zombie Phone with a tablet... '010 Voice Phishing' is prevailing”, accessed on May. 05, 2022, https://www.hankyung.com/article/2022050557301

[3] Junho Ahn et al., “Preventing Voice Phishing Using CMC Call Analysis and Detection”, CISC-S, Busan, 2022.