마스크롬 펌웨어 복원 예측을 위한 시계열 신경망 학습방법 연구

김대원, 이상수, 강동호
한국전자통신연구원

{dwkim77, sangsu, dhkang}@etri.re.kr

A Study on Training a Time-series Neural Network for Predicting Mask ROM Firmware Restoration

Daewon Kim, Sang-su Lee, and Dongho Kang
Electronics and Telecommunications Research Institute

요 약

임베디드 시스템 펌웨어 내 백도어 및 취약점 관련 보안위협이 증가하고 있다. 펌웨어 보안성 분석이 필요하지만, 원본 펌웨어 획득이 쉽지 않으며, 특히 MCU(Micro Controller Unit) 내부 펌웨어는 그 획득난도가 높다. MCU 마스크롬 펌웨어의 경우, 비공개 저장방식으로 비트 셔플링되어 있어, 현재의 수작업 방식으로는 추출된 비트정보로부터 원본 펌웨어 복원에 한계가 있다. 이 문제에 대한 AI기반 자동복원을 위해, 본 논문은 마스크롬 펌웨어 복원 예측을 위한 시계열 신경망 학습방법에 대한 연구를 소개한다.

Ⅰ. 서론

임베디드 시스템들은 펌웨어에 점점 다양한 기능들을 탑재하고 있어, 백도어 및 취약성이 포함될 위협도 높아지고 있다. 사전 분석이 필요하지만, 시스템 내 원본 펌웨어 획득에는 기술적 어려움이 있다. 특히, MCU내 마스크롬으로부터 원본 펌웨어 바이너리를 복원하는 것은 현재의 반복된 수작업으로는 한계가 있다.

최근 전 세계 군, 경찰, 국방 등에서 널리 사용되는 TETRA(Terrestrial Trunked Radio) 통신장비 마스크롬 펌웨어에 심각한 보안 취약점[1](CVE-2022-25333)이 발견되었다. Snowden 유출 기밀문서[2] 등을 통해 TETRA 통신 도청관련 오랜 의혹에 대한 기술적 가능성이 제기된 것이다. 우려되는 점은, 마스크롬 펌웨어에 대한 보안분석 인식 및 펌웨어 복원기술 부족으로 별다른 검증없이 임베디드 시스템들을 사용하고 있다는 점이다.

주사전자현미경(Scanning Electronics Microscope, SEM)을 통해 마스크롬 영상정보로부터 펌웨어를 구성하는 0, 1 비트정보를 추출하는 기술들이 연구되었다[3, 4]. 그러나 추출비트들은 알려지지 않은 방식으로 셔플링되어 있어 현재의 수작업을 통한 원본 펌웨어 조립은, 투입되는 시간, 인력, 비용 등에 비해 그 성공률 한계가 있다.

연구팀은 반복된 수작업 복원 문제를 해결하기 위해, AI기반 자동복원 연구를 진행중이며, 이전 연구들[5, 6]에 이어 본 논문에서는 마스크롬 펌웨어 복원 예측을 위한 시계열 신경망 학습방법에 대한 연구를 소개한다.

Ⅱ. 기술배경

2.1 마스크롬 펌웨어 바이너리 복원 문제

펌웨어는 마스크롬에 저장될 수 있으며, 그 바이너리는 그림 1과 같이 마스크롬 별 회로규칙에 의해 비트 셔플링되어 저장된다. 공급망 보안관점에서, 현재 임베디드 시스템 내에 있는 펌웨어와 시스템 제작사의 공개 펌웨어가 같다는 보장이 없으며, 제작사도 모르는 취약점이 펌웨어에 존재할 수 있다. 펌웨어 특성상, 코드의 재사용이 활발하기 때문에 취약점 존재를 모른 채 수년간에 걸쳐 다양한 제품들에 유사한 펌웨어들이 사용될 확률이 높다. 따라서, 시스템 내 펌웨어 바이너리를 복원해야 백도어 및 취약점 분석을 할 수 있지만, 비트화된 저장규칙이 알려져 있지 않아, 수작업을 통한 경험적인 복원에 의존하고 있으며, 그 복원 성공률도 낮다.

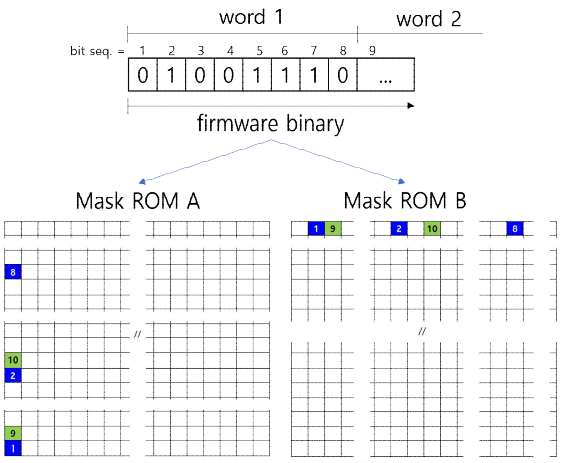

그림 1. 비트 셔플링된 마스크롬 내 펌웨어 비트 예

2.2 이전 연구들

연구팀은 마스크롬 펌웨어 수작업 복원 한계를 극복하기 위해, AI 기반 복원방안을 연구중이다. 본 연구는 chip 집적도 등의 회로제약으로 인해, 비트 셔플링도 마스크롬 물리적 특징 제약하에 있을 확률에 기반한다.

마스크롬 비트정보 추출, 자동복원을 위한 전체구성, 물리적 파라메터, 및 비트선택 순서 리스트 등과 관련한 고려사항들에 대한 연구[5]가 선행되었다. 이후, chip(MCU) 및 마스크롬 물리적 특징 파라메터화, 신경망 학습

활용방안, 및 복원사례 비교를 통한 복원예측 가능성에 대한 결과[6]를 보여주었다.

Ⅲ. 마스크롬 펌웨어 복원예측을 위한 시계열 신경망 학습방법 연구

지난 연구[6]는 물리적 특징들이 유사한 마스크롬들에 저장된 비트화된 펌웨어들은, 그 바이너리 복원방법이 유사할 가능성을 보여주고 있다. 또한, 연구팀은 복원을 위해 비트를 순서대로 선택 및 조립해야 하는 점에 집중하여 시계열 신경망 활용을 고려하였다.

그림 2는 이와 관련하여, 마스크롬 펌웨어 복원예측을 위한 시계열 신경망 학습용 데이터를 보여준다.

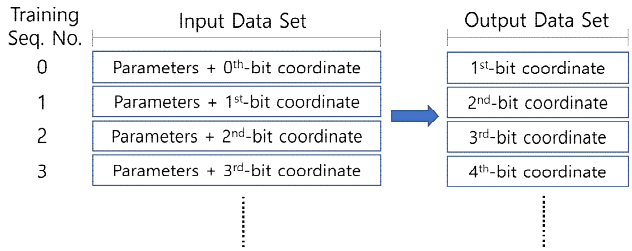

그림 2. 신경망 학습용 데이터

그림 2에서 학습용 데이터는 입력 데이터 세트(Input Data Set)와 출력 데이터 세트(Output Data Set)로 구성된다. 입력 데이터 세트는 파라메터 정보(parameters)와 좌표정보(coordinates)들로 구성된다. 입력 데이터 세트의 파라메터 정보는 chip 및 마스크롬의 물리적 정보를 수치화한 정보들로서, 그 중 마스크롬의 레이아웃 정보는 필수적으로 포함하고 있으며, 다른 물리적 정보들은 학습 및 복원예측 성능을 고려하여 선택될 수 있다.

표 1은 파라메터 정보의 일부인 마스크롬 레이아웃 정보 및 관련 설명의 예를 보여준다.

표 1. 마스크롬 레이아웃 정보 예

항목	설정 예	설명
BitDecoderPos	1	비트 디코더 위치 (ex. 1: Left)
WordDecoderPos	4	워드 디코더 위치 (ex. 4: Bottom)
WordBits	8	바이너리로 변환되는 비트 수
Endianness	1	ex. 1: Big, 2: Little
ExtractedWidth	512	추출된 비트정보의 가로 비트 수
ExtractedHeight	512	추출된 비트정보의 세로 비트 수
BitBlock	32	비트 디코더 상의 비트블록의 개수
BitPerBitBlock	16	비트 디코더 상의 비트블록당 비트 수
WordBlock	1	워드 디코더 상의 비트블록의 개수
BitPerWordBlock	512	워드 디코더 상의 비트블록당 비트 수

그림 2에서 출력 데이터 세트는 학습 시퀀스(Training Seq. No.)별 입력 데이터에 대한 출력되어야 할 정보로서, 최소한 비트선택 좌표인 column 및 row 정보를 포함한다. 해당 좌표들은 입력 데이터 세트 파라메터에 해당하는 마스크롬의 펌웨어를 복원하기 위해 그림 1과 같이 비트를 선택하는 순서 좌표이다.

그림 2에서 학습 시퀀스별 입력 데이터에 대해 출력 데이터가 예측되도록 신경망이 반복 학습된다. 입력 데이터 세트의 입력좌표와 출력 데이터 세트의 출력좌표가 연결되어 학습되는 것으로, 시퀀스 0의 초기 입력좌표(0, 0)로 시작된 좌표예측이 실패하였을 경우, 물리적 특징 관련 다른 초기좌표로 다른 예측을 수행할 수 있게 된다. 따라서, 마스크롬 비트정보의 펌웨어 바이너리 복원예측을 위해, 제안한 방법으로 학습된 시계열 신경망을 이용한다면, 초기좌표에 변화를 주어 새로운 예측결과를 도출할 수 있다. 이를 통해 사람의 반복적인 복원시도를 신경망이 대신하게 된다.

표 2는 입력 및 출력 데이터 세트의 좌표정보로 이용되는 비트선택 순서관련 비트 시퀀스 정보의 예를 보여주고 있다. 그림 1과 연관 지어, seq는 비트선택 순서, word는 워드번호, col과 row는 추출된 비트정보에서 비트를 선택하는 좌표를 의미한다.

표 2. 비트 시퀀스 정보 예

seq	word	col	row
1	1	0	511
2	1	0	447
3	1	0	383
4	1	0	319
5	1	0	255
6	1	0	191
7	1	0	127
8	1	0	63
9	2	0	510
…	…	…	…

Ⅳ. 결론 및 향후 연구방향

본 논문은 마스크롬 펌웨어 복원예측을 위한 시계열 신경망 학습방법에 대한 연구를 보여준다. 복원을 위한 비트선택 순서의 중요성에 집중하여, 물리적 특징인 파라메터와 비트선택 시퀀스 정보를 시계열 신경망에 학습하는 방법을 제안한다. 학습된 신경망은 입력 초기좌표를 변화시켜, 기존 수작업 복원보다 높은 성공 확률을 기대할 수 있는 다양한 복원예측 결과를 유도해 줄 수 있다. 학습에 사용할 마스크롬 복원정보를 구하는 것은 어려운 일이며 보유한 학습정보를 증가시킬 방안, 파라메터 정보를 함축할 방안, 및 좋은 학습결과를 보여줄 수 있는 신경망 모델에 대한 연구가 향후 진행될 필요가 있다.

ACKNOWLEDGMENT

이 논문은 2024년도 정부(과학기술정보통신부)의 재원으로 정보통신기획평가원의 지원을 받아 수행된 연구임. (NO. RS-2020-II200215, 시스템/디바이스의 하드웨어 공급망 위협 대응 핵심기술 개발)

참 고 문 헌

[1] Carlo Meijer et al., “All Cops Are Broadcasting: Breaking TETRA After Decades in the Shadows,” Black Hat USA, 2023.

[2] The Intercept_, “NSA Telegraph: SIGDEV Efforts in Support of the United Nations Framework for Climate Change Conference, Bali, Indonesia,” Aug. 15, 2018.

[3] S. E. Quadir, J. Chen, D. Forte, N. Asadizanjani, S. Shahbazmohamadi, L. Wang, J. Chandy, and M. Tehranipoor, “A survey on chip to system reverse engineering,” ACM journal on emerging technologies in computing systems (JETC), vol. 13, no. 1, pp. 1- 34, 2016.

[4] C. Gerlinsky, “Bits from the matrix: Optical ROM extraction”, Presentation, Hardwear.io, USA, 2019.

[5] 김대원 외, “마스크롬 펌웨어 비트정보의 자동화된 바이너리 복원 연구,” 한국 인공지능 학술대회, pp. 384-385, 2023.

[6] 김대원 외, “마스크롬 복원 신경망 학습 데이터 구축을 위한 물리적 특징 분석,” 한국통신학회 하계학술대회, pp. 1956-1957, 2024.