마스크롬 복원 신경망 학습 데이터 구축을 위한 물리적 특징 분석

김대원, 이상수, 강동호
한국전자통신연구원
{dwkim77, sangsu, dhkang}@etri.re.kr

An Analysis of Physical Features for Constructing Neural Network Training Data for Mask ROM Restoration

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

요 약

MCU(Micro Controller Unit) 마스크롬(Mask ROM) 펌웨어 내 백도어 및 취약성 관련 보안 위협이 증가하고 있다. 펌웨어는 마스크롬에 임의의 규칙으로 비트화 저장되어 있어, 비트정보를 원래의 펌웨어 바이너리 형태로 복원하는 것은 어려운 문제이다. 현재 마스크롬 복원은 역공학 인력의 수작업 분석에 의존하고 있으며, 투입되는 인력, 비용, 시간 대비 복원 성공률도 낮다. 본 논문은 신경망을 통한 마스크롬 복원 자동화를 위해, MCU 및 마스크롬 물리적 특징을 신경망 학습에 활용하는 방안을 소개한다.

Ⅰ. 서론

드론/IoT/국방 등 다양한 분야에서 임베디드 시스템 사용이 증가하고 있다. 임베디드 시스템의 기능은 주로 펌웨어 형태로 구성되어 있어, 펌웨어 보안 위협의 심각성도 함께 증가하고 있다[1]. 최근엔 군, 경찰, 국방 등의 보안 통신에 사용되는 TETRA(Terrestrial Trunked Radio) 통신장비 마스크롬 내 임의코드를 실행할 수 있는 취약점이 발견되어, 도청 가능성이 제기되었다[2].

임베디드 시스템 내 펌웨어 위협을 분석하기 위해서는 펌웨어 바이너리 획득이 필요하지만, 기술적으로 쉽지 않은 문제이며, 특히 MCU 내부 펌웨어 접근은 그 난도가 더욱 높다. MCU 내부 펌웨어 접근은 글리칭(glitching)이라는 오류주입(fault injection) 기술을 사용해 볼 수 있으나, 글리칭이 실패하면 MCU를 분해하여 마스크롬 펌웨어 획득시도를 해보아야 한다.

MCU 패키지 분해(decapping) 및 레이어들을 제거(delayering)해 가면서 마스크롬 레이어에 도달하면, 주사전자현미경(Scanning Electronics Microscope) 등을 통해 영상정보를 획득하고, 영상의 음영 차이를 통해 펌웨어 바이너리의 비트화된 0, 1 정보를 획득한다[3]. 비트정보는 역공학 인력의 수작업 분석을 통해 펌웨어 바이너리 복원을 시도하고 있지만, 비트화된 저장규칙이 알려져 있지 않기 때문에, 투입되는 인력, 시간, 비용 대비 복원 성공률이 낮다.

연구팀은 기존의 반복된 수작업 복원 시도 문제를 해결하기 위해, AI기반 복원 자동화 방안에 관해 연구하고 있으며[4], 본 논문에서는 신경망을 통한 마스크롬 복원 자동화를 위해, MCU 및 마스크롬 물리적 특징을 신경망 학습에 활용하는 방안을 소개한다.

Ⅱ. 본론

그림 1은 신경망을 통한 마스크롬 복원 자동화의 개념을 보여준다. MCU 및 마스크롬의 물리적 특징 기반 파라메터 정보와 마스크롬 복원을 위해 비트를 선택해 나가는 비트 선택 순서정보인 비트 시퀀스 정보를 신경망에 학습한다. 복원 요청받은 마스크롬에 대해 학습된 신경망을 통해 비트조합 순서예측, 예측오차에 대한 후처리 기술적용, 바이너리 생성, 바이너리 검증, 및 피드백 단계로 복원예측이 루어진다.

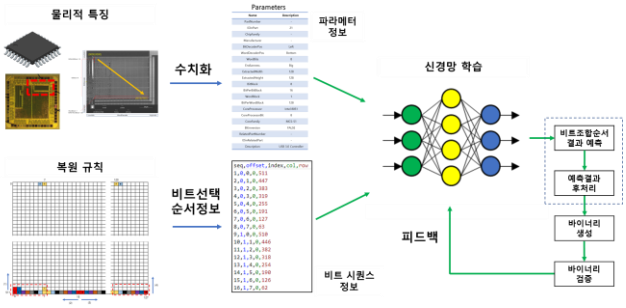


그림 1. AI 기반 마스크롬 자동복원 개념도

표 1은 회사명 및 제품명 등을 익명으로 한, 실제 마스크롬의 물리적 특징을 파라메터 정보로 활용하는 예를 보여준다.

표 1. 물리적 특징 기반 파라메터 정보 예

분류	항목	설정 예
식별정보	PartNumber	PN1
	IDinPart	21
레이아웃 정보	BitDecoderPos	Left
	WordDecoderPos	Bottom
	WordBits	8
	Endianness	Big
	ExtractedWidth	128
	ExtractedHeight	128
	BitBlock	8
	BitPerBitBlock	16
	WordBlock	1
	BitPerWordBlock	128
보조정보	ChipFamily	CF
	Manufacturer	MF
	RelatedPartNumber	PN
	IDinRelatedPart	12
보완정보	CoreProcessor	Intel 8051
	CoreProcessorBit	8
	CoreFamily	MCS-51
	BitInversion	FALSE
기타정보	Description	USB 3.0 Controller

다양한 복원예측을 할 수 있도록 많은 물리적 특징들을 수치화하는 것이 좋으며, 신경망을 어떻게 활용하느냐

에 따라 표 1의 전체정보가 학습될 수도 있고, 신경망 부분 학습정보, 빠른 복원방법 선택정보, 및 복원예측 정책정보 등으로 활용될 수 있다. 아래는 파라메터 정보들의 특징을 설명한다.

▌식별정보

복원 요청받은 마스크롬의 식별정보와 동일한 것이 복원 시스템에 있다면 신경망을 거치지 않고 저장된 복원 시퀀스 정보로 복원한다. MCU(PartNumber) 내에는 여러 개의 마스크롬 영역이 있을 수 있으며, 이를 구분하기 위해 IDinPart를 정의한다. 예) col=2, row=1 위치

▌레이아웃 정보

마스크롬 주변의 디코더 위치(BitDecoderPos 및 WordDecoderPos), 마스크롬의 크기(ExtractedWidth 및 ExtractedHeight), 비트정보의 블록구분 상태(BitBlock: BitDecoder 방향 블록 개수, BitPerBitBlock: 비트 블록당 비트 수, WordBlock, 및 BitPerWordBlock), 워드를 구성하는 비트 수(WordBits), 및 Endianness 정보를 포함하고 있다. 기본적으로 신경망에 학습되는 정보이다.

▌보조정보

신경망을 통한 예측에 도움을 줄 수 있는 정보들이다. 마스크롬의 레이아웃 정보가 같거나 유사하더라도 복원 규칙은 대부분 다를 수 있다. 그러나, MCU가 칩 계열(ChipFamily)이나 제조사(Manufacturer)가 같다면 같은 복원규칙을 사용할 확률이 높다. 복원할 마스크롬과 복원 방법이 같은 정보(RelatedPartNumber 및 IDinRelated-Part)를 파악하여 신경망을 거치지 않고 저장된 복원 시퀀스 정보로 복원하던가, 신경망의 예측 정책으로 활용할 수 있다.

▌보완정보

WordBits나 Endianness 등이 확인되지 않을 때, MCU 내부 프로세서 정보(CoreProcessor, CoreProcessorBit, CoreFamily)를 통해 해당 정보를 유추할 수 있다. BitInversion은 선택된 비트를 반전시켜야 하는지를 나타낸다.

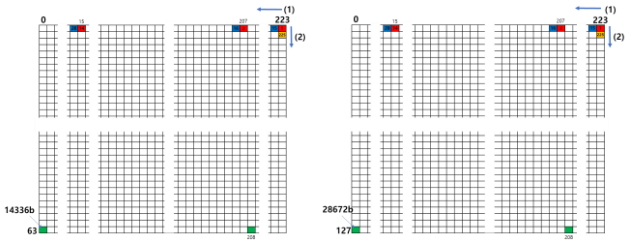
Ⅲ. 복원 사례 비교

표 2는 유사한 파라메터를 갖는 A, B 두 개의 다른 마스크롬의 파라메터 정보이다. 마스크롬을 직접 분해하거나 관련 문서들을 확보하지 않는 한, 대부분 표 2와 같은 일부정보만 파악할 수 있다. 특이사항은 레이아웃 정보 내 ExtractedHeight가 다른 상황에서, 칩 계열 및 제조사 정보가 같음을 정책에 반영하여 신경망을 통해 같은 복원규칙을 유도할 수 있다는 점이다. 이는 파라메터와 복원 시퀀스를 학습하여 복원을 예측하는, 본 연구의 의도를 나타내는 결과이다.

표 2. 유사한 파라메터를 갖는 마스크롬 A, B

항목	마스크롬 A	마스크롬 B
PartNumber	PnA	PnB
WordBits	14	14
Endianness	Big	Big
ExtractedWidth	224	224
ExtractedHeight	64	128
ChipFamily	CF	CF
Manufacturer	MF	MF
Description	USB to UART	USB to UART

그림 2는 마스크롬 A(왼쪽), B(오른쪽)의 비트선택 순서 도식, 워드를 구성하는 비트선택 순서(BitSeq), 및 비트선택 순서에 따른 좌표(col, row) 선택 경향을 보여준다. (a)에서 두 마스크롬 모두 (1) 첫 줄에서 (0, 223) 좌표부터 (0, 0) 방향으로 14비트씩을 선택하고, 첫 줄이

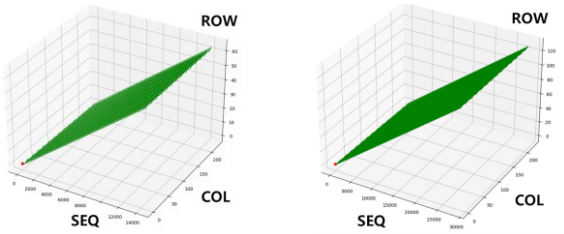


(a) 도식화된 비트선택 순서

Color	Word(14b)	BitSeq
	1	1 ~ 14
	2	15 ~ 28
	17	225 ~ 238
	1024	14323 ~ 14336

Color	Word(14b)	BitSeq
	1	1 ~ 14
	2	15 ~ 28
	17	225 ~ 238
	2048	28659 ~ 28672

(b) 워드를 구성하는 비트선택 순서(BitSeq) 및 색상표



(c) 비트선택 순서(sequence)에 따른 좌표(col, row)선택 경향

그림 2. 마스크롬 A(왼쪽), B(오른쪽) 복원 비트선택 분석

모두 선택되면 (2) 다음 줄로 같은 규칙으로 좌표를 선택함을 알 수 있다. 파라메터 정보로 좌표선택 경향을 grouping 하여, 유사한 복원경향 위주로 복원예측을 하도록 (c)와 같은 특징을 신경망에 반영할 수도 있다.

Ⅳ. 결론 및 향후 연구방향

본 논문에서는 신경망을 통한 마스크롬 복원 자동화를 위해, MCU 및 마스크롬 물리적 특징을 파라메터화 하여 신경망 학습에 활용하는 방안을 소개하였다. 본 논문은 유사한 파라메터의 마스크롬들이 신경망을 통해 개연성 있는 복원예측의 가능성이 있음을 보여준다. 향후, 물리적 특징인 파라메터와 비트선택 순서를 나타내는 비트 시퀀스 정보를 어떻게 신경망에 학습할지에 관한 연구가 필요하다.

ACKNOWLEDGMENT

이 논문은 2024년도 정부(과학기술정보통신부)의 재원으로 정보통신기획평가원의 지원을 받아 수행된 연구임. (NO. 2020-0-00215, 시스템/디바이스의 하드웨어 공급망 위협 대응 핵심기술 개발)

참 고 문 헌

[1] Eclypsium, “firmWar: An Imminent Threat to the Foundation of Computing,” Black Hat Asia, 2023.

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

[3] C. Gerlinsky, “Bits from the matrix: Optical ROM extraction”, Presentation, Hardwear.io, USA, 2019. Davies R. W." The Data Encryption standard in perspective," Computer Security and the Data Encryption Standard, pp. 129-132.

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