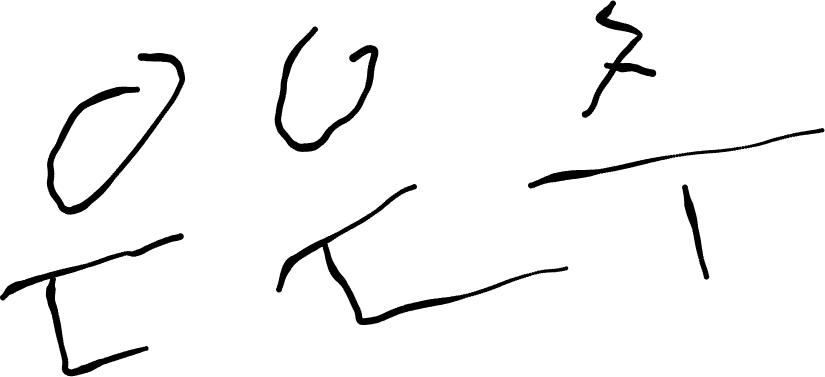
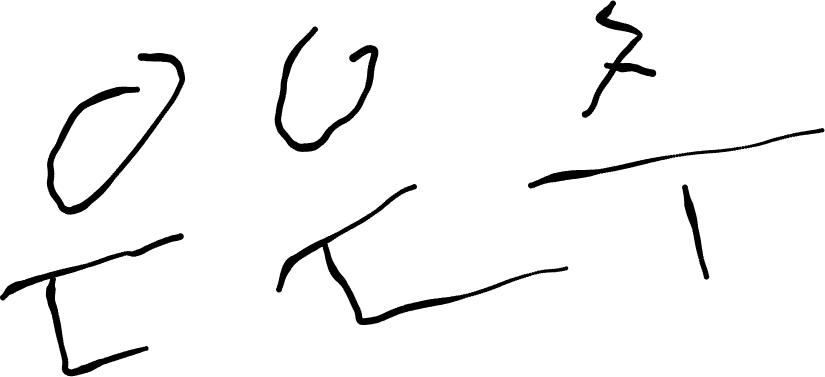
|  |
| --- |
|  |
| 2024 제2회 KISIA 정보보호 개발자 해커톤 개발 기획서 |
|  |

|  |  |
| --- | --- |
| **팀명** | Maxwell |
| **개발 주제** | AI 텍스트분석을 이용한 리버스 엔지니어링 툴 |

|  |
| --- |
| **□ 개발 배경 및 의도** |
| 리버스 엔지니어링을 수행하는 것은 프로그램의 작동 방식, 내부 구조, 그리고 잠재적인 보안 위험 요소를 깊이 있게 파악할 수 있는 중요한 방법론이다. 이를 통해 사용자는 프로그램이 실제로 어떤 방식으로 동작하는지, 어떤 기능을 수행하는지, 그리고 프로그램 내에 숨겨진 악성 코드나 보안 취약점이 존재하는지를 명확히 이해할 수 있다. 하지만, 리버스 엔지니어링은 고도의 기술적 지식과 경험을 요구하는 분야로, 이 과정에 대한 진입 장벽이 매우 높다. 어셈블리 언어와 같은 저수준 프로그래밍 언어에 대한 이해도, 운영체제의 시스템 구조에 대한 깊은 지식, 그리고 이를 활용한 분석 도구의 숙련된 사용이 필수적이기 때문이다. 따라서 이러한 복잡한 과정을 처음 접하는 사용자들에게는 학습이 매우 까다롭고 시간이 많이 소요되는 작업이 될 수밖에 없다.  특히 프로그램의 내부를 단순히 들여다보고자 하는 사용자, 즉 특정 기능이나 잠재적인 위험 요소를 간단하게 파악하려는 사용자에게 리버스 엔지니어링의 개념을 숙지하고 관련 도구를 사용하는 방법을 익히는 것은 지나치게 과도한 요구로 느껴질 수 있다. 실제로 이러한 전문성을 요구하지 않는 사용자들은 프로그램의 내부를 간단히 분석하거나, 잠재적인 위험 요소를 식별하고자 할 뿐이지, 깊이 있는 리버스 엔지니어링 지식을 필요로 하지는 않는다.  시중에 나와 있는 보안 프로그램들도 파일 분석 기능을 제공하지만, 이들 프로그램이 사용자에게 제공하는 정보는 제한적일 때가 많다. 예를 들어, 대부분의 보안 소프트웨어는 파일의 기본적인 안전성에 대해 평가하고, 악성 코드의 존재 여부를 판단할 수 있는 기능을 제공한다. 그러나 이러한 프로그램들은 일반적으로 표준화된 패턴이나 알려진 악성 코드 서명을 기반으로 작동하며, 비표준 파일 포맷이나 새로운 유형의 위협에 대해서는 유연하게 대처하기 어려운 경우가 많다. 더욱이, 이러한 분석 결과는 일반 사용자에게는 지나치게 기술적이거나 불충분한 정보로 느껴질 수 있다.  이러한 문제점을 해결하기 위해 이 프로그램의 주된 목표는 LLM(Large Language Model)을 활용하여 리버스 엔지니어링 과정을 자동으로 수행하고, 그 결과를 사용자에게 자연어로 제공하는 것이다. LLM은 대규모 언어 모델로, 방대한 텍스트 데이터를 학습하여 인간과 같은 자연스러운 언어 생성 능력을 갖추고 있다. 이 프로그램은 기드라(Ghidra)와 같은 리버스 엔지니어링 도구를 통해 파일의 내부 코드를 분석하고, LLM을 통해 그 분석 결과를 자연어로 해석하여 사용자에게 전달한다. |
| **□ 개발 계획** |
| 1. 기드라와 LLM을 연결하는 파일 분석 자동화 프로그램 스크립트  기드라와 LLM을 연결하여 파일 분석을 자동화하는 프로그램은 다음과 같은 과정을 거친다. 먼저, 파이썬 스크립트를 통해 기드라를 호출하여 분석할 파일을 디스어셈블 및 디컴파일한다. 이를 통해 함수 목록, 코드 패턴, 메모리 매핑, 특정 API 호출 내역 등 세부 정보를 추출한다. 이러한 정보는 리버스 엔지니어링 과정에서 핵심적인 데이터로, 프로그램의 내부 구조와 잠재적 위험성을 파악하는 데 필수적이다. 추출된 데이터는 JSON 형식으로 저장되며, 이 JSON 데이터는 LLM에 전달할 수 있도록 포매팅된다. JSON 형식은 구조화된 데이터를 효율적으로 전달할 수 있어, LLM이 필요한 정보를 쉽게 처리하고 분석할 수 있도록 한다.  2. LLM의 파인튜닝  LLM(예: GPT-4)을 사용하여 자연어로 파일 분석 결과를 제공하기 위해서는 사전 학습된 모델을 파인튜닝해야 한다. 기본적으로 GPT-4는 광범위한 자연어 데이터를 학습한 상태로 제공되지만, 리버스 엔지니어링 도메인에 대한 특화된 학습은 이루어지지 않은 상태다. 따라서 LLM이 리버스 엔지니어링과 관련된 코드 패턴, 함수 호출, 그리고 잠재적인 악성 코드 행위와 정상적인 프로그램 동작을 구분할 수 있도록 추가 학습이 필요하다.  파인튜닝 과정에서는 악성 코드의 코드 패턴, 함수 호출 등의 정보를 정상 코드와 비교 분석한 데이터를 모델에 제공하여 학습시킨다. 이를 통해 모델은 악성 행위의 특징을 인식하고, 정상적인 프로그램 동작과 구분하는 능력을 갖추게 된다. 이러한 학습 데이터셋에는 실제 악성 코드 사례와 정상 코드 사례가 포함되며, 이들 간의 차이점을 명확히 이해할 수 있도록 구성된다. 파인튜닝이 완료된 후, 모델은 테스트 코드를 사용하여 성능을 검증한다. 이 과정에서 모델이 정확하게 악성 코드를 식별하고, 자연어로 명확한 설명을 제공할 수 있는지를 평가하여 모델의 성능을 피드백한 후조정을 통해 최적화한다.  3. 사용자 친화적 GUI와 채팅 인터페이스  사용자는 GUI 내에서 클릭 앤 드롭(Drag and Drop) 방식으로 분석할 파일을 업로드할 수 있다. 파일이 업로드되면, 자동으로 분석이 수행되며, 그 결과가 GUI를 통해 사용자에게 제공된다.  GUI 내에는 채팅 형식의 인터페이스가 포함되어 있다. 사용자는 이 채팅 인터페이스를 통해 분석 결과에 대해 추가적인 질문을 하거나, 더 자세한 설명을 요청할 수 있다. |
| **□ 모델·서비스 활용성** |
| 이 프로그램은 보안 전문가와 전혀 지식이 없는 일반인 그 사이를 타겟팅한다. 리버스 엔지니어링 또는 기타 보안에 대한 지식이 없으나 잠재적 위험이 있는 파일을 다운받아서 사용할 여지가 있는 개발자, IT관리자, 또는 기술에 관심이 있는 사람에게 도움이 될 수 있다. 이러한 사람들은 복잡한 보안 도구나 리버스 엔지니어링 기법을 익히지 않아도 프로그램을 통해 파일의 안전성을 검사할 수 있다. 특히 개발자들은 인터넷에서 검증되지 않은 다양한 라이브러리나 오픈소스 소프트웨어를 다운로드하는 경우가 많은데, 이 경우 안전성을 확신할 수 없는 경우가 많다. 이 프로그램을 통해 개발자들은 자신이 진행하는 프로젝트의 보안을 강화하고, 취약점을 미리 판단하여 발생할 수 있는 위험을 사전에 방지할 수 있다.  더해서, 보안 공부를 시작하는 학생이나 보안에 관심이 있는 일반 사용자에게도 이 프로그램은 유용할 수 있는데, 리얼월드의 프로그램을 직접 분석하는 것은 어렵기 때문에, AI의 답변을 가이드라인처럼 이용하여 공부하는 데에도 이용할 수 있다. |
| **□ 기대 효과·사회적 효과** |
| *이 프로그램의 가장 근본적인 기대 효과는 대상이 누구가 되었건 리버스 엔지니어링에 대한 장벽을 낮추고 프로그램을 분석할 수 있게 하는 것이다. 리버스 엔지니어링은 어셈블리 언어에 대한 이해도와, 운영체제의 시스템 구조에 대한 이해도도 요구되므로 직접 툴을 이용해 분석하는 것은 어려운 일이다. 또한, 이러한 프로그램 분석에 대한 진입장벽을 낮춰, 보안 지식이 없는 개인 이용자뿐만 아니라 비용이나 인력 문제로 전문적인 보안 인프라를 갖추기 어려운 중소기업의 경우에도 이 프로그램을 보안 위협 탐지 도구로 활용할 수 있다. 이를 통해 사용자들은 프로그램의 위험성을 툴을 통해 직접 파악할 수 있게 되고, 외부의 도움 없이도 일정 수준의 사전 예방 조치는 취할 수 있게 된다.* |

※ 참고문헌

팀장 : 은은수()

팀원 : 은은수()

팀원 : (인)

팀원 : (인)

**한국정보보호산업협회장 귀하**

□ 개인벙보 수집ㆍ이용 동의서

|  |
| --- |
| 개인정보 수집ㆍ이용 동의서  **가. 개인정보의 수집·이용에 관한 사항**  □ 개인정보의 수집·이용 목적  ○ 본 대회 운영에 따른 공지 및 자료조사  □ 수집·이용할 개인정보의 항목  ○ 전화번호, 주소, 생년월일, 성별, 이메일, 소속 등 참가신청 및 대회 운영 중 취득한 정보  □ 개인정보의 보유·이용기간  ○ 개인정보는 원칙적으로 개인정보의 수집 및 이용목적이 달성되면 지체 없이 파기합니다. 단, 본 대회 종료 후 참여 인정문서 발급 및 차년도 행사 준비를 위한 역대 수상자 정보공유 등을 위한 최소한의 자료(성명, 전화번호, 이메일)는 보존됩니다. (보존기간 : 대회 종료 후 5년)  □ 동의를 거부할 권리 및 동의를 거부할 경우의 불이익  ○ 위 개인정보의 수집·이용에 거부할 권리가 있음을 알려드립니다.  단, 수집항목은 사업 진행을 위한 최소한의 필수정보로서 개인정보 수집·이용에 동의하지 않으실 경우 대회 참가 및 제반활동이 불가능합니다.  **나. 개인정보 제3자 제공에 관한 사항**  □ 제공받는 자  ○ 과기정통부, ㈜스틸리언(2024 제2회 KISIA 정보보호 개발자 해커톤 행사 운영 용역사),(주)제이앤아이글로벌(2024 제2회 KISIA 정보보호 개발자 해커톤 행사 운영 용역사)  □ 제공받는 자의 목적  ○ ‘2024 제2회 KISIA 정보보호 개발자 해커톤’ 진행 및 운영, 참가자 관리  □ 제공하는 개인정보 항목  ○ 전화번호, 주소, 이메일, 소속 등 참가신청 및 프로그램 운영 중 취득한 정보  □ 동의를 거부할 권리 및 동의를 거부할 경우의 불이익  ○ 위 제3자에 대한 개인정보의 제공에 관한 동의를 거부할 수 있으나 본 대회 참가를 위해 필수적이므로, 위 사항에 동의하셔야만 참가 및 활동이 가능합니다.  **본인은 본 동의서의 개인정보 수집·이용·제공에 관한 권리 및 내용을 이해했으며, 위와 같은 목적으로 본인의 개인정보를 수집·이용 및 제3자에게 제공하는 것에 동의합니다.**  2024년 8월 4일  참 가 자 : 은은수 ()  **한국정보보호산업협회 귀중** |

□ 명예 서약서

|  |
| --- |
| 명예 서약서  □ 팀 명 : Maxwell  □ 성 명 : 은은수  상기 본인은 과학기술정보통신부에서 주최하고 한국정보보호산업협회에서 주관하는『2024 제2회 KISIA 정보보호 개발자 해커톤**』**에 참가함에 있어 다음의 사항을 서약합니다.   * 다 음 -   ○ 참가 안내사항 및 참가자 유의사항을 충분히 숙지했으며 이해하고, 순조로운 진행을 위해 협조하겠습니다.  ○ **해커톤에서 개발한 결과물 등이 타인의 도움을 사전에 받아 제작했거나 부정한 방법으로 수상한 경우에는 수상이 취소되고 참가자는 상장 및 상금 반환됨을 동의**합니다.  ○ 대회 진행 간 개발과정 및 결과물이 촬영될 수 있고, 자료로 남겨지거나 공개적으로 게시될 수 있다는 것에 동의합니다.  ○ 심사결과에 승복하겠으며, 정정당당히 대회에 임하겠습니다.  ○ **사실에 입각한 자료만을 제출**하며, 제출내용 중 **허위사실로 밝혀질 경우 당 대회는 물론 기관에서 수행하는 여타의 사업에 대한 참여제한** 등의 조치에 대해 감수하겠습니다.  ○ 수상자로 결정됨에 따라 언론사 등에 사업아이템 등이 공개됨에 동의하며, 향후 지식재산권 등 수상 관련 민원에 대한 법적 책임을 지겠습니다.  ○ 사업 관련, 확인되지 않은 사실을 유포 시, 법적·도의적 책임을 지겠습니다.  2024년 8월 4일  참 가 자 : 은은수 ()  **한국정보보호산업협회 귀중** |