주간 활동 보고서-0321

산업보안학과 32200492 김명현

3/15~19

2주차에 진행한 주제 선정 Brainstorming에서 관심 있는 주제를 하시는 분이 있어 이름을 적었는데 적은 인원으로도 가능하다고 하셔서 혼자 프로젝트를 진행하게 되었습니다. 그때 급하게 생각했던 주제는 다음과 같습니다:

Dynamic link 방식으로 프로그램이 만들어지면 라이브러리를 하나의 메모리에 매핑하고 여러 프로그램이 공유하면서 사용을 합니다. 이때 라이브러리가 외부에 있기 때문에 함수의 주소를 알아오는 과정이 필요한데 이때 plt/got를 참조하여 함수를 호출합니다. 평문을 암호화시키기 위해서 RSA같은 비대칭 암호보다는 block cipher(AES, DES, 3DES...)를 자주 사용할텐데 여기서 사용하는 암호 라이브러리(openssl)의 함수들도 예외가 아닙니다. Code injection을 통해 참조하려는 암호 라이브러리의 함수 주소를 제가 만든 임의의 코드 주소로 바꿔 함수를 하이재킹합니다. 대부분의 암호화 함수의 파라미터는 비슷한 위치(평문은 첫번째 인자, 키는 두번째 인자)에 위치하고 있기 때문에 레지스터에 저장되는 값들을 추출해온다면 평문을 추출할 수 있을 것 같습니다. 따라서 암호화 함수를 스킵하고 평문과 키를 추출할 수 있다라는 게 결론입니다.

위 주제로 기대할 수 있는 효과는 암호화를 무력화할 수 있다는 점입니다. 상대 PC에 있는 파일들을 암호화하여 접속 권한을 빼앗고 되찾고 싶으면 랜섬을 지불하라고 요구하는 멀웨어인 랜섬웨어를 무력화할 수 있을 것 같습니다.

3/20~21

하지만 위 프로젝트를 혼자 한학기만에 진행하기는 어렵다고 판단해서 이번 수업의 주제로써 포기하고 여유롭게 따로 해보기로 결정했습니다.

그래서 따로 생각한 주제는 "매끄럽고 자연스러운 번역을 가능하게 해주는 프로그램"입니다. 기존에 있는 구글, 파파고의 번역기들도 성능이 좋지만 제가 경험해봤을 때, 표현하고자 했던 표현들이 구글 번역기나 파파고로 돌렸을 때 뭔가 부자연스러운 부분이 없지 않아 있었습니다.

따라서 구글 번역기에 돌린 1차 번역판을 chatgpt를 활용해 교정한다면 더욱 자연스러운 문장으로 번역할 수 있습니다. 따라서 구글 번역 오픈소스를 이용하여 한글을 입력받고 이것을 chatgpt에게 open API로 요청하여 교정을한 후 응답을 받는다면 고급 번역기를 만들 수 있을 것 같습니다.

구글 번역관련

https://py-googletrans.readthedocs.io/en/latest/

https://cloud.google.com/translate/docs/basic/translating-text?hl=ko

chatgpt 관련

https://teddylee777.github.io/python/chatgpt-blog-automation/