컴퓨터공학부 캡스톤디자인 중간평가 답변서

팀명: 5 조 assist(a security safety important special team)
조원: 손현기 (조장), 김주환, 김호준, 오예린, 이동윤, Ruslan

심사의견
기존의 소프트웨어가 불분명하다고 판단한 파일을 입력으로 받는 것인데, 일반적으로 기존 소프트웨어가 불분명하다고 판별한 파일 중 어느 정도의 비율이 악성코드로 판별되는지를 제시하여 이 소프트웨어의 필요성을 명확히 하면 좋겠음.
답변
새로운 보안위협에 대응하기 위해 각 보안기업에서 운용하는 시큐리티대응센터는 신종 악성코드에 대한 보고서와 악성코드에 대한 통계 제공하지만, 전문가가 검사한 파일의 수와 검사한 파일 중 악성코드의 수를 별도로 제공하고 있지는 않습니다. 따라서 해당 비율을 확인하기 어렵습니다. 본 프로젝트의 목표는, 기존 소프트웨어의 결과와 상관없이, 입력 파일 중 악성 행위를 수행할 것으로 예상되는 부분을 요약함으로써 전문가의 분석 시간을 줄이는 것입니다. 저희는 필요성을 보이기 위해 제안서에 전문가의 악성코드 분석 시간이 짧게는 수 시간에서 길게는 수 주가 걸린다는 인터뷰 결과를 인용함으로써 새로운 보안위협에 빠르게 대응하기 위해서는 전문가의 분석 시간을 줄이기 위한 소프트웨어가 필요함을 제시했습니다.

심사의견 & 질문
제안하는 방법이 얼마나 좋은 성능을 내는지를 보여줄 수 있을만한 객관적인 평가 방법 마련 필요 ‘악성 부분’에 대한 gold standard 를 확보하고 있는지? 확보할 방법은?
답변
제안된 소프트웨어 asi 의 성능을 객관적으로 측정하기 위하여 전문가의 악성코드 분석 결과와 asi 의 분석 결과를 비교할 예정입니다. 즉, 각 함수에 대한 전문가의 평가와 asi 의 판단을 비교했을 때, 전문가가 악성이라 분류한 함수에 대해 asi 가 높은 확률로 악성 행위를 수행할 것이라 판단하고, 악성이라 분류하지 않은 함수에 대해 asi 가 낮은 확률로 악성 행위를 수행할 것이라 판단한다면 제안된 프로그램이 좋은 성능을 갖는다고 평가합니다. 요컨대, 악성 부분에 대한 gold standard 는 기존 전문가의 악성 코드 분석 보고서를 사용하고, asi 의 성능에 대한 평가를 위해 전문가의 보고서와 asi 의 판단 결과를 비교합니다.

심사의견
‘전문가를 돕는 악성 부분 탐지’가 목표이지만, 악성 부분을 탐지한다는 것은 악성 파일도 탐지 가능하다는 것으로 보임. → 기존의 악성파일 탐지방법의 성능과 비슷한 성능까지는 보여줘야 ‘악성 부분 탐지’도 의미가 있을 것으로 보임
답변
제안된 소프트웨어를 응용하여 파일의 악성/정상 여부를 판정할 수도 있습니다. 그러나, 이를 악성파일 분류 문제를 해결하기 위해 학습시킨 신경망과 비교하는 것은 적합하지 않다고 생각합니다. 제안된 소프트웨어는 각 함수의 악성/정상 여부를 점수화하는 것이므로 악성파일 분류만을 위해 학습된 신경망과 비교하면 성능이 낮을 수밖에 없습니다. 즉, 제안된 프로그램을 응용하여 악성파일 분류를 할 수는 있지만, 이 목적만을 위해 학습을 시킨 신경망과 성능을 비교하는 것은 적절치 않을 것으로 생각합니다. 대신, 두 번째 심사의견에 답변 드린 것처럼 asi 의 성능을 객관적으로 측정하기 위해 전문가의 보고서와 asi 의 판단 결과를 비교할 예정입니다.

심사의견
실험 결과를 보면, 정상파일에서 이상탐지를 오히려 더 많이 하는 문제가 있음. 해결방안 필요.
답변
1 차 중간보고서의 [그림 15]의 y 축은 이상탐지한 파일의 수가 아니라 이상탐지한 함수의 개수입니다. [그림 16]에서 볼 수 있듯, 실제 이상탐지된 함수가 없는 파일의 비율은 정상 파일이 더 많으므로 본 소프트웨어가 적절히 분류를 수행한다고 볼 수 있습니다. 현재는 10,000 개의 적은 데이터에 대해서만 학습을 수행했기 때문에 분석 성능이 떨어지는 것으로 보입니다. 향후 더 많은 데이터에 대해서 학습한다면 이러한 오류를 줄일 수 있을 것으로 기대합니다. 추가로, 현재는 어셈블리 코드의 니모닉만을 이용해 학습을 수행하는데, 향후 각 니모닉의 피연산자를 추가해 특징벡터를 생성함으로써 분석 성능을 높일 예정입니다.

질문
기존 악성코드 분석 프로젝트와의 차별점이 무엇인가?
답변
기존 프로젝트는 파일의 정상/악성 여부를 판별하는 것을 목표로 했습니다. 본 프로젝트는 파일의 정상/악성 여부를 판단하는 것이 아니라, 각 함수의 악성 행위 수행 여부를 점수화 함으로써 전문가의 분석을 돕는 프로그램을 만드는 것입니다.