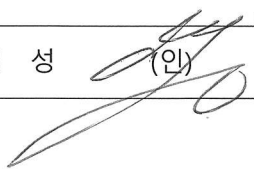


캡스톤디자인 면담 확인서

팀원	2013104053 김동준, 2013104129 한선우, 2016110312 송미희, 2014104110 신기성		
주제	IoT 디바이스 펌웨어 취약점 탐지 방법의 비교 분석		
면담일시	2019. 6. 3.	지도교수	조 진 성 (인) 
면 담 내 용	<ul style="list-style-type: none"> ● 발표를 위해 탐지 시나리오를 구성하고 시연을 준비할 것. ● 정적분석 부분에서는 오탐이 많은 단점을 보이기 위해 실제 오픈소스 소프트웨어에 대하여 탐지한 결과에 대해서도 참고로 알아두는 것이 필요함. 그러나 전체 탐지방안 제시 시나리오에서 정적 분석이 갖는 역할이 분명히 있음을 강조하고, 퍼징과 기호실행과 상호 보완이 가능하다는 점을 매끄럽게 연결해야 함. 긴 소스코드에 대하여 탐지범위를 제한할 수 있는 힌트를 제공할 수 있는 점을 강조하면 될 것임. ● libFuzzer는 변수를 직접 조작하여 정적분석에서 검출된 취약점을 실제로 잡아내는 시나리오를 제시하면 됨. 그러나 다중 중첩문에 대해선 취약점 검출이 어려우므로 기호 실행과의 연계성을 언급 하면 될 것임. ● AFL의 경우 사용자의 테스트 케이스 입력에 대해서 퍼징이 어떻게 다르게 진행되는지 명확하게 이해하고 적용하는 것이 요구됨. 탐지율을 더욱 높이기 위한 방법을 좀 더 연구해볼 것. ● KLEE는 Path Explosion에 취약하고 코드 커버리지에 강하므로 각 특징을 살릴 수 있는 두 가지 상황을 만들어 소개할 것. 가장 좋은 툴은 존재하지 않고 각 툴의 강점을 모아야 더 큰 시너지를 낼 수 있다는 점을 강조할 것. 		