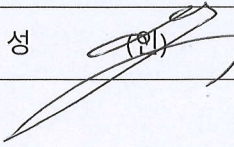


## 캡스톤디자인 면담 확인서

팀원	2013104053 김동준, 2013104129 한선우, 2016110312 송미희, 2014104110 신기성		
주제	IoT 디바이스 펌웨어 취약점 탐지 방법의 비교 분석		
면담일시	2019. 4. 24.	지도교수	조 진 성 (인) 
면 담 내 용	<ul style="list-style-type: none"> <li>● 팀원들 간의 소통 및 협업 강화가 필요함.</li> <li>● 코드 취약점 부분에서는 기존에 선정한 11개의 도구를 모두 쓰는 것은 분석량이 너무 많음. 대상 코드에 적합한 도구로 5개 정도로 추려서 심도 있는 분석을 하는 방향으로 할 것. IoT application이 대부분 c나 c++로 개발되었으므로 해당 언어에 집중된 분석이 요구됨, 또한 동일한 조건에서 비교하는 것이 객관성을 확보하기 용이하므로 본인이 접근하기 편한 windows 기반의 환경에서 실행이 가능한 도구들로 선정할 것. 팀원들 간의 논의를 통해 다른 탐지 방법을 고려한 분석 대상 선택이 필요함. 현재는 bluez코드에 대해서만 모의 분석을 해 보았지만, 퍼징이나 기호실행과의 비교를 위해 더 단순한 취약점 코드에 대해서 3가지 방법을 모두 사용하여 비교해보는 것이 필요함</li> <li>● 오픈소스 기반 프로그램에 대해 퍼징을 실행하고자 화이트박스 기반 퍼징만을 사용하여 각 툴간의 비교가 필요함. AFL 툴에 대한 이해도를 높이고 취약점이 있는 간단한 코드를 활용하거나 실제로 구현해 보고 분석하며 취약점 코드에 대한 이해도를 좀 더 높이는 것이 요구됨.</li> <li>● LibFuzzer의 작동 원리와 결과 이해가 요구되며 오픈소스 기반 프로그램 코드를 돌려보고 다른 툴과의 차이점을 비교 분석하는 것이 필요함.</li> <li>● 기본적인 프로그램 분석을 통해 높은 KLEE의 이해도를 이용해 더욱 복잡한 프로그램을 분석해 보는 것이 요구됨.</li> </ul>		