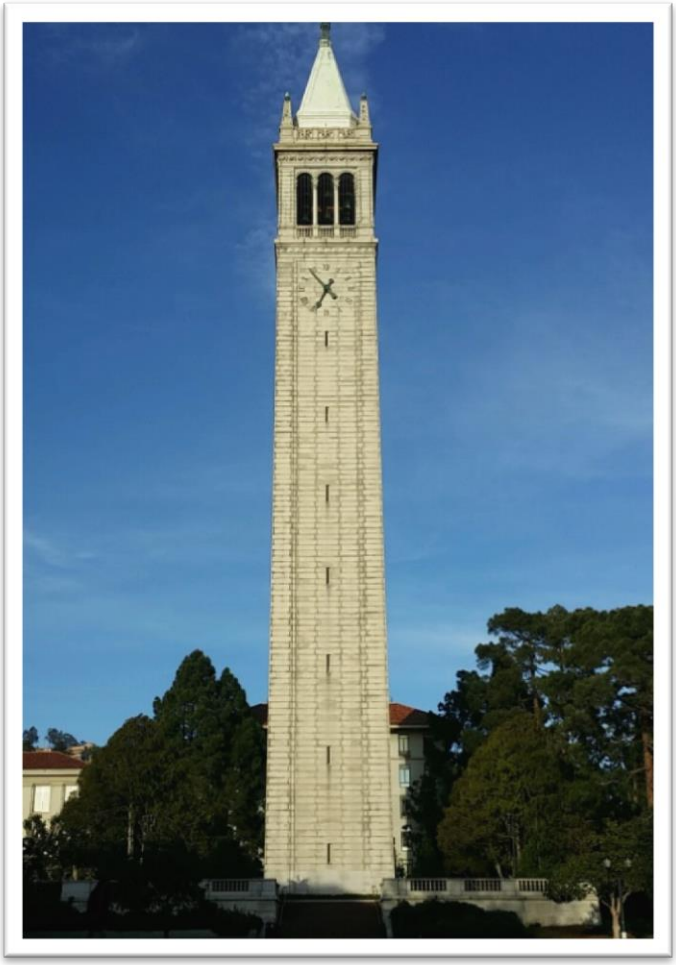
UC Berkeley 교환연구 방문기



Berkeley, California, USA

2015.04.24 - 2015.08.28

최재승

서울대학교 프로그래밍 연구실

들어가며

지난 4월 말부터 8월까지 UC 버클리의 Dawn Song 교수님 연구실에서 방문연구를 진행하였다. 이전부터 Dawn Song 교수님 그룹은 프로그램 분석 기술을 활용하여 컴퓨터보안 분야의 문제를 해결하는데 많은 관심을 가지고 있으셨고, 몇 년 전에 이우석 선배님이 버클리에 방문하여 연구에 참여하기도 하셨다. 이번에도 프로그램 분석 기술과 관련하여 도움을 얻기 위해 우리 서울대 프로그래밍 연구실과 합동 연구를 진행하였으며, 이에 감사하게도 기회를 얻어 버클리에 방문 연구자로 다녀오게 되었다.

Cyber Grand Challenge

내가 UC 버클리에서 방문 연구자로써 맡은 일은 Cyber Grand Challenge라는 일종의 경연(competition)에 참여하는 것이었다. 이 대회는 약 2년에 걸쳐 진행되며, 예선을 통해 선발된 8팀이 2016년 8월에 본선을 치러 우승팀을 가리게 된다.

Cyber Grand Challenge는 소프트웨어의 취약점을 자동으로 발견하여 공격 및 방어하는 시스템을 가지고 경쟁하는 대회이다. 소프트웨어의 규모와 복잡도가 나날이 증가함에 따라 프로그램 취약점을 자동으로 분석하는 기술이 점점 중요해지고 있다. Cyber Grand Challenge는 미 국방성의 연구기관인 DARPA에서 이러한 기술의 발전을 촉진하기 위해 개최한 대회이다.

Cyber Grand Challenge에 참가한 대부분의 팀은 주어진 프로그램의 취약점을 찾기 위해 symbolic execution과 fuzzing을 사용하였다. 이것은 대회의 채점 방식이 실제로 프로그램의 취약점을 공격하는 입력을 생성해야 점수를 부여하는 시스템이기 때문인 것으로 보인다. 다시 말해, 단순히 프로그램의 어느 지점에서 버퍼 오버런이 발생한다는 것을 알아내는 것 만으로는 충분하지 않고, 프로그램을 비정상 종료(crash)시키거나 실행 흐름을 조작(control flow hijack)하는 공격 익스플로잇(exploit)을 생성해야 점수를 얻을 수 있다.

대회에서 분석 및 공격해야 하는 프로그램은 모두 바이너리 실행파일로 주어진다. 정보보안 분야에서는 바이너리 분석을 굉장히 중요하게 생각하는데, 실제로 사용되는 수많은 실제 세계(real-world) 소프트웨어들이 소스 코드 없이 바이너리 실행파일로만 접근 가능하기 때문이다.

CodeJitsu 팀

나는 CodeJitsu팀의 일원으로 Cyber Grand Challenge에 참가하였다. 이 팀은 UC 버클리, 스위스 로잔 연방 공대(EPFL), Syracuse 대학 등 여러 연구 그룹이 연합하여 결성된 팀이다. EPFL 측은 symbolic execution 기술을, Syracuse 대학 측은 퍼징 부분을 담당하였으며, UC 버클리 그룹은 프로그램의 취약점을 보완(hardening)하는 역할을 맡았다.

Codejitsu팀은 6월 3일에 진행된 Cyber Grand Challenge에서 3위를 기록하여 본선에 진출하였다. 앞으로 1년 가량 준비 기간을 거친 뒤 2016년 8월에 본선에 참가하여 다른 7개 팀과 우승을 놓고 겨루게 된다.

Codejitsu 팀 중 UC 버클리 멤버들

내가 속해 있던 UC 버클리 그룹은 프로그램을 보완(hardening)하는 문제를 다음과 같은 방향으로 접근하였다. 우선 주어진 바이너리 실행파일을 LLVM IR로 번역한 다음, LLVM IR 상에서 프로그램을 안전하게 고친다. 그 다음 수정된 LLVM IR을 clang으로 컴파일하여 다시 바이너리 형태의 파일을 얻을 수 있다. 프로그램의 보완(hardening)은 오류를 일으킬 수 있는 명령 앞에 간단한 체크를 추가하는 것으로 이루어졌다. 예를 들어, 메모리 읽기/쓰기 명령의 경우 우선 포인터 값이 유효한 주소인지 체크하고, 유효하지 않은 주소일 경우 그대로 안전하게 종료하도록 만든다.

나의 역할은 LLVM IR로 표현되어 있는 바이너리를 분석하는 분석기를 구현하여, 다른

그룹들에게 유용한 정보를 제공하는 것이었다. 우선, 분석기는 요약 해석에 기반하여 프로그램을 안전(sound)하게 분석하고, 잠재적인 오류/취약점을 찾아내서 알람을 생성한다. 이 정보는 프로그램 명령을 선별적으로 hardening하는 데 활용될 수 있으며, symbolic execution이 취약점 공격 익스플로잇(exploit)을 생성하는 과정에서 힌트로 활용될 수도 있다.

컴퓨터공학부 건물 "Soda Hall"

연구 분위기, 느낀 점

Dawn Song 교수님 그룹은 정적 분석을 이론적으로 깊게 이해하는 것 보다는, 그것을 도구 삼아 보안 분야의 다양한 문제를 다루는데 집중하는 경향이 있었다. 어떻게든 잘 돌아가는 툴이 구현되기만 한다면, 그 툴이 어떤 기초 위에 어떤 방식으로 설계되었는지 크게 신경 쓰지 않는다. 대신 그렇게 구현된 툴을 수많은 테스트 케이스에 대해 실험해 보는 것을 중요하게 여겨, Jenkins 와 같은 테스트 프레임워크를 구축해 두고 수시로 dry-run 을 실시하였다.

기초가 탄탄하지 않은 채로 일이 인행되는 점은 다소 아쉬웠다. '가장 이론적인 것이 가장 실용적인 것이다' 라는 말이 있듯이, 튼튼한 이론적 토대 위에서 출발한

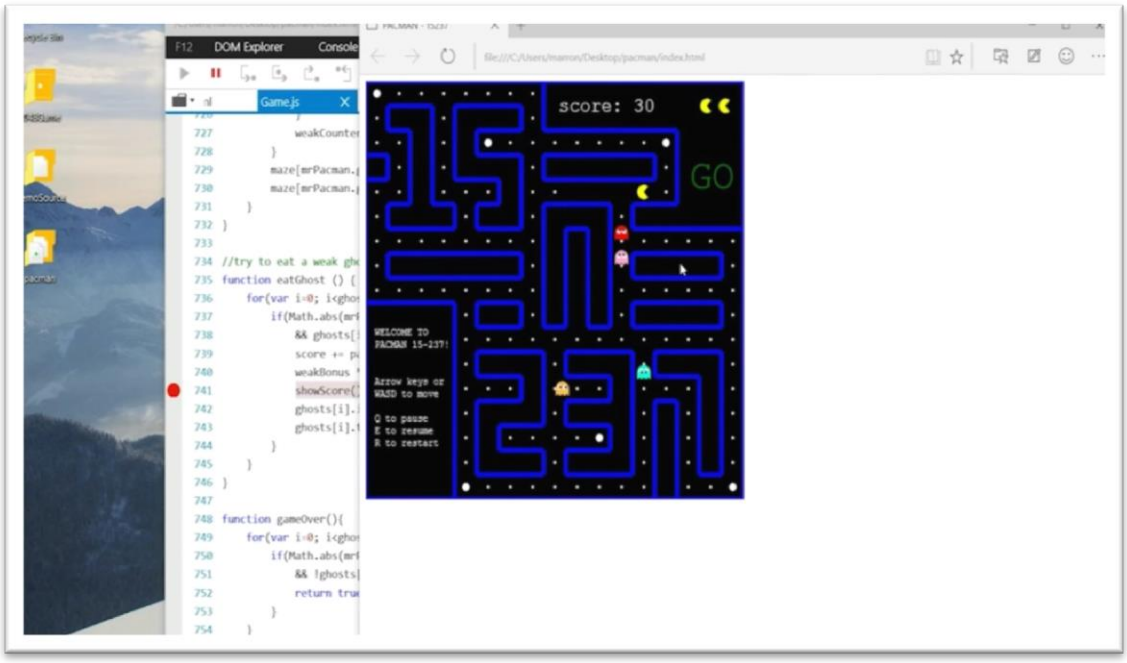
툴이야말로 정말 일류의 툴이 될 수 있다고 생각하기 때문이다. 튼튼한 이론의 반석에서 출발해서 실용적으로 훌륭한 툴에 도달할 수 있다면 가장 좋을 것이다.

Dawn Song 교수님 연구실에 있는 동안 보안 분야에서 어떤 문제가 중요시되고 있는지, 그 동향을 많이 들을 수 있었던 것은 좋은 기회가 되었다. 프로그램 분석 기술을 활용해서 접근해 보고 싶은 문제가 몇 개 있었는데, 다소 버거워 보이기는 하지만 앞으로의 연구에 있어 좋은 도전 거리가 될 것 같다.

세미나

버클리에서 열리는 세미나는 흥미로운 것들이 많았는데, 도착하고 몇 주 지나지 않아 종강하고 방학이 시작되면서 세미나가 많이 열리지 않았던 점은 아쉽다. 특별히 인상 깊게 들었던 세미나들은 아래와 같다.

Time Travelling Debugging for HTML/Javascript



Time Traveling Debugging 시스템으로 팩맨 게임을 디버깅하는 시연

이 발표는 개발자가 프로그램의 실행 흐름을 앞뒤(forward-backward)로 자유롭게 돌아다니면서 디버깅할 수 있도록 하는 기술에 대하여 다루었다. 프로그램의 실행 과정을 거슬러 올라가면서 살펴볼 수 있다면 디버깅이 수월해질 것이다. 지금까지 시도된 구현들은 실행시간의 오버헤드가 매우 높아 실용적이지 못했는데, 이 연구의 구현

체는 MS의 Edge 브라우저에서 실행되는 javascript 앱에 대하여 10% 이내의 실행 시간 오버헤드를 보이는 시스템을 구현했다.

눈에 보이는 확실한 프로토타입 구현체를 가지고 와서 중간중간에 보여준 데모가 인상적이었다. 간단한 장난감 사이즈 프로그램이 아니라, GUI 인터페이스 및 사용자와의 상호작용도 있는 규모 있는 프로그램에서도 TTD 시스템은 안정적으로 잘 작동하였다. 엔지니어링에 많은 노력을 기울여 좋은 도구를 만들어낸 연구라는 인상을 받았다.

Rail Traffic Services Oriented Mobile Communication

이 발표는 TGV나 신칸센과 같은 고속 열차(High Speed Railway, HSR)를 위한 통신 시스템에 대하여 소개하였다. 고속 열차를 안전하게 운행하기 위해서는 중앙 관제 시스템과 열차, 그리고 철로에 설치된 회로 사이에 원활한 통신이 이뤄져야 한다. 이를 위해서는 고속으로 운행하는 열차와 안정적으로 통신할 수 있어야 하기 때문에, GSM 이라는 모바일 통신 표준에 기반하여 통신 시스템을 구축한다.

고속 열차의 통신 시스템은 생각보다 복잡한 요소들로 이루어져 있으며 그 시스템에서는 다양한 문제가 발생한다. 철로에 설치된 측정장치와 열차에 탑재된 컴퓨터, 그리고 중앙관제센터는 열차의 속도와 다음 열차까지의 거리와 같은 다양한 데이터를 활발하게 주고받는다. 이 과정에서, 통신을 해야 하는 열차는 고속으로 이동하며, 터널과 같은 장애물이 있어도 통신이 가능해야 한다는 문제가 있다. 통신 시스템이 이러한 문제를 제대로 해결하지 못하고 오작동하는 바람에 실제 열차 사고로 이어진 경우도 빈번하다.

Security in the real world (case study of password manager)

이 발표에서는 여러 상용 비밀번호 관리(password manager) 시스템에서 취약점들을 발견한 케이스 스터디를 통하여, 실제 소프트웨어 개발 현장에서 어떤 보안 취약점이 일어날 수 있으며 소프트웨어 보안에 대해 어떻게 접근해야 하는지에 대해 설명하였다.

비밀번호 관리 시스템은, 사용자가 하나의 강력한(strong) 마스터 비밀번호만 기억하고 있으면, 사용자가 가입하는 사이트의 비밀번호 생성 및 로그인 과정을 처리해 주는 시스템이다. 이러한 시스템을 설계하고 구현하다 보면 여러 취약점이 발생할 수 있으며, 이 발표에서는 인증 취약점, UI 취약점, 웹 접속 취약점 등이 다루어졌다.

대형 소프트웨어 개발사에서 보안을 담당한 경험을 가진 발표자가 전해주는 여러 메시지 중에 흥미로운 것들이 많이 있었다. 예컨대, 소프트웨어 제품을 개발할 때 보안 취약점의 발견은 일찍 취해지면 취해질수록 비용이 적게 소모된다는 메시지나, 개발자는 자신의 코드가 언제나 악의적인 공격의 대상이 될 수 있다는 것을 자각하고 있어야 한다는 메시지가 그랬다.

생활

방문연구로 가 있는 4개월 동안 미국에서의 생활에 적응하는 것도 큰 일이었다. 생활과 관련하여 기록할 만한 것들은 아래와 같다.

음식

다양한 국적의 학생들이 모여 살기 때문에, 버클리에서 접할 수 있는 음식은 제법 다양하다. 햄버거나 샌드위치 같은 패스트푸드, 멕시코 음식, 베트남 음식 등을 자주 먹었고, 괜찮은 한식당도 버클리 근처에 여러 군데 있다. 가끔 스테이크를 먹을 기회도 있었는데, 한국에 비해 저렴한 가격에 질 좋은 고기를 먹을 수 있다.

보통 아침, 점심은 저렴하고 간단하게 먹을 수 있는 시리얼이나 샌드위치 등으로 해결했으며, 저녁은 학생식당이나 버클리 인근의 한식당을 애용하였다. UC 버클리의 학생식당은 서울대의 학생식당과는 조금 다른데, 서울대에 비해 비싼 가격(7~8달러)을 받는 대신 다양하고 질 좋은 음식이 나온다.

UC 버클리 학생식당의 음식

교통

UC 버클리의 교통 관리국에서 버스 정기권을 구입하면, 버클리에서 큰 불편함 없이 돌아다닐 수 있다. 정기권 가격은 1년에 400달러 정도이며, 매년 7월에 1년치를 구입한 다음 귀국할 때 남은 기간에 비례한 금액을 돌려받는다. 버스 정기권을 구입하면 원래 1달러 요금을 받는 학교 셔틀버스도 자유롭게 사용할 수 있다.

버클리에서 샌프란시스코나 공항 등으로 이동할 때에는 BART라는 열차를 이용하는 것이 편하다. 배차 간격을 잘 맞춰 가면 40분 정도 걸려서 샌프란시스코에 도착할 수 있다. 아쉽게도 BART는 산 호세 및 실리콘밸리 지역까지는 닿지 않는다.

주거

UC 버클리의 방학 기간에 얼추 맞춰 방문 연구를 간다면, 서브렛을 통해 비교적 저렴하게 집을 구할 수 있다. 서브렛은 집에 세를 들어 사는 사람으로부터 다시 집을 임대하여 짧은 기간 동안 지내는 것이다. 방학 동안 고국으로 돌아가 시간을 보내는 UC 버클리의 학생들이 보통 집을 서브렛으로 많이 내놓는다. craiglist.co.kr나 샌프란 한인 커뮤니티에 이러한 매물이 많이 올라오는데, 다소 번거롭기는 했지만 유심히 살펴보고 있다 괜찮은 조건의 집을 구할 수 있었다.

주거지를 찾는 과정에서 캠퍼스에서 너무 남쪽으로 내려가면 치안이 급격히 악화되므로 주의해야 한다. 버클리 시는 남쪽에 오클랜드와 경계를 맞대고 있는데, 오클랜드는 미국에서 치안이 안 좋고 강력 범죄가 많기로 손에 꼽히는 위험한 도시이다.

관광

4개월이라는 연구 기간이 촉박하다 보니, 시간을 내어 주변의 도시를 충분히 다녀보지 못했던 점이 조금 아쉽다. 샌프란시스코에 두어 번 정도 방문한 것이 다였는데, Pier39나 유람선 등 무난한 관광지가 제법 있어 가끔 여유를 갖는데 도움이 되었다. 관광지는 아니지만, UC 버클리의 캠퍼스 자체도 전원적이고 운치가 있어 거닐기에 좋다. 연구 및 개발을 하다 막히는 부분이 있으면 잠시 산책을 하며 생각을 정리하곤 했다.

마치며

4개월이라는 짧은 시간이었지만, 많은 것을 경험하고 생각해볼 수 있는 좋은 기회였다. 방문 연구자로 있는 동안 만족할 만큼 잘하지 못해서 아쉬움도 많이 남지만, 지금부터라도 부족한 점들을 채워나가 실력을 갖추고 싶다.

유익한 경험을 할 수 있는 기회를 주고 지원해 주신 이광근 교수님께, 그리고 방문 연구를 위한 절차를 도와주신 행정팀에 깊이 감사드린다. 방문하기 전부터 여러 조언을 해 주신 이우석 선배님, 그리고 버클리에 머무는 동안 여러모로 도와주신 최원태 선배님에게도 감사드린다.