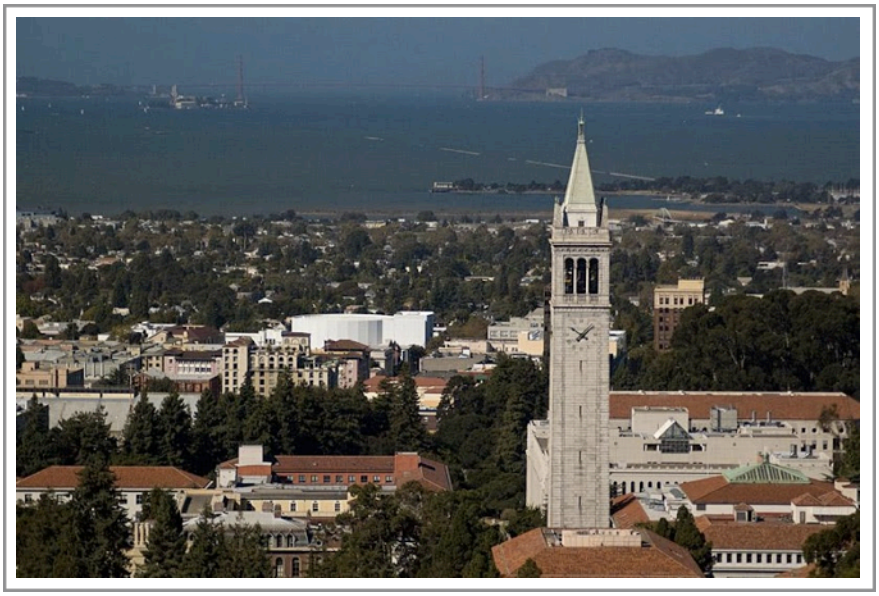
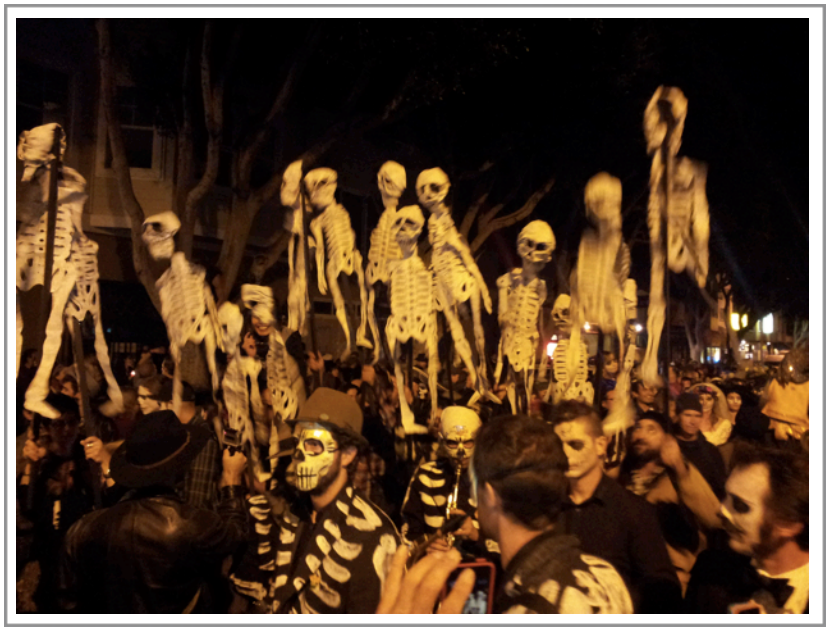




UC Berkeley 방문기

Berkeley, CA, USA

7월 30일 ~ 11월 19일

서울대학교 프로그래밍 연구실

이우석

미국 UC Berkeley의 Dawn Song 교수님 그룹에 약 네 달간 방문연구를 다녀왔다. 거기서 드로이드블레이즈 라는 안드로이드 보안관련 프로젝트라는 수행했다. 프로젝트의 목표는 안드로이드 앱에 대해서 정적/동적 분석을 수행하여 나쁜 앱인지 아닌지 결과를 도출하는 분석기를 만드는 것이다.

프로젝트 리더인 Dawn Song 교수님은 이 프로젝트 연구성과를 가져다 사업화할 계획을 갖고 있기 때문에 일차적인 목표가 연구보다는 실용적인 도구를 만드는 것에 있었다. 내가 있었던 때는 한창 연이어 잡힌 데모 스케쥴로 바쁜 때였다. 팀 구성원들은 매일매일 미팅을 하고, 데모 전까지 분석기가 돌아가게 하기 위해서 고군분투했다. 한 차례의 데모가 끝나도, 다음 데모가 또 잡혀있었기 때문에 일이 쉼 없이 돌아갔다.

스패로우에 이어서 실용적인 정적분석 만들기에 일조할 수 있는 경험을 가질 수 있었던 것은 좋았지만, 새로운 연구 주제를 찾아 진행하기는 어려운 분위기였다. 그렇지만 다국적 팀에서 여러 사람들과 호흡하며 일하면서 배운 것들은 연구 못지 않게 중요했다는 생각이 든다.

드로이드블레이즈 소개

드로이드 블레이즈는 임의의 안드로이드 앱에 대해서 나쁜 앱으로 의심되는 정도와 그 근거를 보고하는 시스템이다. 앱이 하는 나쁜 짓들은 다양한데, 사용자 몰래 사생활 정보를 빼내어 원격 서버로 보내거나 유료 문자나 전화를 걸거나, 루트 권한을 따내거나, 다른 나쁜 앱을 기존 앱의 업데이트를 가장하여 설치하거나 하는 등이다. 드로이드블레이즈에는 정적 분석, 동적 분석, 기계 학습 분야의 기술들이 통합되었다. 일차적인 목표가 연구보다는 실용적인 도구를 만드는 것에 있기 때문에 정교하고 수준 높은 기술보다는 간단한 기술들이 결합된 것이 특징이다. 프로젝트는 아직 진행중에 있고, 나도 귀국하고 나서도 계속 그 팀에 속해서 일하고 있다.

웹 UI 에 사용자가 앱 파일을 업로드하면 동/정적 분석이 수행된 결과와 나쁜 앱일 가능성이 점수로 표현된다. 정적분석은 커버리지가 높고(안드로이드의 복잡한 특성 상 분석의 안전성은 얻기 어렵지만) 동적분석은 커버리지가 낮지만 정확한 관찰사실을 사용자에게 알려줄 수 있기 때문에 둘 다 쓰인다. 아직은 아니지만 동/정적 분석이 서로에게 피드백을 주면서 상보적인 관계에서 분석이 진행되는 형태의 분석도 계획 중에 있다. 아래는 분석결과 페이지의 모습이다.

APK file: ADRD-4015.apk
Suspicious behaviors: 20
Using dynamic results: true
Threat level: 10/10

Summary of behaviors

Category	Threat Score
CODE_SIMILARITY	10
SMS_SENDING	2
SENSITIVE_INFORMATION	10
OBFUSCATION	6
NETWORK	0
FILESYSTEM	6

CODE_SIMILARITY

Threat	Behavior	Stat.	Dyn.	Confidence
high	Match to malware family: ADRD/Geinimi	✓		
				(Category threat level: 10/10)

SMS_SENDING

Threat	Behavior	Stat.	Dyn.	Confidence
low	SMS sending (dst: UNKNOWN, text: UNKNOWN)	✓		
				(Category threat level: 2/10)

SENSITIVE_INFORMATION

Threat	Behavior	Stat.	Dyn.	Confidence
high	Sensitive information updated (Preferred APN)	✓		
high	Sensitive information read (Preferred APN)	✓		

정적분석과 동적분석에서 앱의 행동들이 추출되고, 각 행동 별로 위험점수가 표현된다. 점수 도출 부분은 간단한 Bayesian classifier 로 구현되어있다. 600여개의 나쁜 앱과 500여개의 나쁘지 않은 앱들에서 도출된 동/정적 분석 결과가 학습에 쓰였다.

정적 분석은 사용자 몰래 유료 SMS나 전화를 거는지, 확인되지 않는 앱을 설치하는지, 어떤 네트워크 호스트에 접근하는지 등등 나쁜 앱 판별에 실용적으로 쓰일 수 있는 여러가지 정보를 간단한 분석으로 도출한다. 다양한 정적 의미 분석들이 희종이형과 원찬이형이 만든 정적분석 프레임워크 코러스 위에 구현되어 있다.

동적분석은 앱이 동적으로 어떤 파일들을 접근하는지, 어떤 시스템 콜이나 API들을 호출하는지 등을 알아낸다. 정적 분석과 달리 프레임워크 위에 구현된 것은 아니어서 구현이 확장성있게 되어있는 것은 아니다.

나는 민감한 정보가 외부로 유출되는지 판단하는 테인트 분석을 비롯해서 그 외 몇 가지 다른 간단한 정적분석들을 구현했다.

연구 분위기

연구 분위기상 내게 신선했던 것은 크게 두 가지였다. 매우 짧은 주기로 진행상황을 보고해야 했던 것과, 일이 기초가 탄탄하지는 않게 빠르게 진행됐던 점이다. 진행상황을 보고해야 했던 주기는 처음에는 1주간격, 나중에는 하루간격, 심지어 30분간격이 되기도 했다.

내가 간 처음 한달 정도는 매주 한번 미팅을 했다. 각자 돌아가면서 한 주 동안 한 일을 설명하고 맞닥뜨린 문제들을 설명했다. 시시콜콜한 얘기를 하기에는 내 영어실력이 많이 미천했기 때문에 빨리 결과를 내서 내가 한 일이 무엇인지 그래프나 표로 한방에 보여주는 편이 좋았다. 그러다보니 첫 몇주는 본의아니게 다른 사람들보다 일을 많이하는 것 같기도 했다.

이 프로젝트의 데모 일정들이 잡히면서부터는 스케쥴이 빡빡하게 돌아가기 시작했다. 미팅도 매일했는데, 날마다 각자 순서대로 1~2분동안 어제 무엇을 했고, 오늘은 무엇을 할 것인지 말하는 시간을 가졌다. 처음에 난 이런형식의 미팅에 스트레스를 많이 받았다. 왜냐하면 비교적 자잘한 문제들과 해결책들에 대해서도 힘든 영어로 굳이 소통해야 했기 때문이다 (하루동안의 진척은 사소한 경우가 대부분이다). “그냥 어제하던거 계속했다” 라고만 말하면 안되고 좀 더 자세하게 얘기 해야했다. 부족한 영어가 큰 문제였는데, 영어를 잘하는 다른 사람들과 달리 나는 말할 내용을 미리 짧게라도 연습해야 했다. 일의 진척을 내느라 연설(?)준비를 미처 못하면, 내가 말할 차례가 올 때 까지 가슴이 쿵쾅쿵쾅 뛰고 긴장이 되었다. 버벅거리고 실수 투성이로 미팅을 마치면 마음이 괴로웠다. 별거 아닌거 같아도 이걸 매일하니 스트레스가 이만저만이 아니었다.

나는 이런 형식의 미팅이 쓸데없는 시간 낭비인데다가 중장기적인 계획을 막는다고 생각했다(다른 팀원들도 대체로 매일하는 미팅에 대해서 부정적이었다). 그래도 피할 수가 없어서 꾸역꾸역하다 보니 적응이 되었다. 그리고 짧은 주기의 보고의무를 견디면서 일이 너무 빠르고 허술하게 되지 않게 관리하는 능력이 필요하다는 걸 깨달았다. 왜냐하면 앞으로 또 이렇게 짧은주기의 보고를 요구하는 보스를 만나지 않으리란 보장이 없고, 그에 휘둘리지 않고 일을 제대로 해내려면 이런 상황에 대한 대처능력이 필요할 것이기 때문이다. 그렇게 나름 긍정적으로 생각하다보니, 세부적인 문제와 해결방법을 얘기하는데도 어느정도 익숙해졌다. 말하는 연습은 자전거를 타고 출근하는 중얼중얼 거리면서 했다. 나중에는 일의 진행사항을 말할 때 많이 자신감이 붙었다. 결과적으로는 나름 좋은 경험이 되었던 것 같다.

데모 스케쥴이 임박해서는 하루단위의 진행상황 보고는 짧은 주기도 아니었다. 어떤 날은 Dawn 교수님이 돌아다니시면서 거의 30분 단위로 진행상황을 체크하기도 했다. 이것 또한 처음엔 적응이 안돼서 교수님을 피해서 화장실로 대피하기도 했다. Dawn 교수님이 그렇게 자주 체크했던 것은 주로 각자가 현재 해야하는 일을 정확하게 알고 하고있는지였다. 누가

잘 이해 못하고 있다 싶으면 바로 잡아주거나 관련된 사람들을 불러 모아 얘기하게 하였다. 잘못된 의사 전달로 인한 시간낭비를 막는 것을 프로젝트 관리의 지상목표로 삼으신 듯 했다. 회의를 할 때도 내용이 너무 세부적으로 간다 싶으면 끊고, 일을 적임자에게 할당하는 데 능했다.

데모 몇주 전부터는 주말에도 자주 회의를 하고(비록 회의 내용은 주말에 해야할 만큼 급한게 전혀 아니긴 했지만) 평일에도 새벽에 퇴근하기도 했다. Dawn 교수님을 비롯, 팀 구성원들의 일에 대한 열정을 엿볼 수 있었다.

그렇지만 기초가 탄탄하게 일이 진행되기보다는 일단 돌아가는 것을 빨리 만드는 식으로 일이 진행된 것은 좀 아쉽다. 결과를 빨리빨리 내야하다보니 문제가 생겨도 근본적인 해결책을 생각하기 보다 미봉책으로 메꾸어지기도 했고, 인터페이스가 바뀌면 코드 대공사가 일어나기도 했다(요약의 경계를 지키며 코딩하기에 시간이 촉박했기 때문에).

이들은 솔루션이란 case by case 의 집합이라는 생각이 강한 듯 하다. 그래서 이들은 대단위 실험을 하여 가능한한 많은 코너 케이스를 다룰려고 한다. crawling 하여 모은 수 만개의 안드로이드 앱에 대해서 분산시스템에서의 실험을 수행하기도 했다. 하룻밤새 수백~수천개의 앱을 테스트하고, 낮동안 분석기가 중단된 경우의 로그들을 살펴보고 빨리 해결한 다음, 다시 수백~수천개의 앱을 밤새 테스트 하는 과정이 반복되었다.

생활

세미나

버클리에서는 좋은 세미나 발표가 많았다. 인상깊었던 것 중 하나는 수학과에서 열린 logic colloquium 이었는데, 미분방정식을 위한 논리체계, 자연어 의사소통을 표현한 논리구조에 대한 발표들을 들었다. 질문하는 버클리 학생들의 영민함, 위트를 엿볼 수 있었고, 발표를 들으러 온 전설적인 학자들(william craig, dana scot, martin davis 등)도 직접 볼 수 있었다. (웹페이지 http://logic.berkeley.edu/events.html에 발표 슬라이드와 요약을 찾아볼 수 있다) 또한 점심을 공짜로 주는 보안 세미나, 박사 후 연구원들이 일반인 대상으로 하는 발표들, 유명 학자들의 초청 발표들에 몇번 참가하여 좋은 발표들을 들을 수 있었다.

ESL 수업

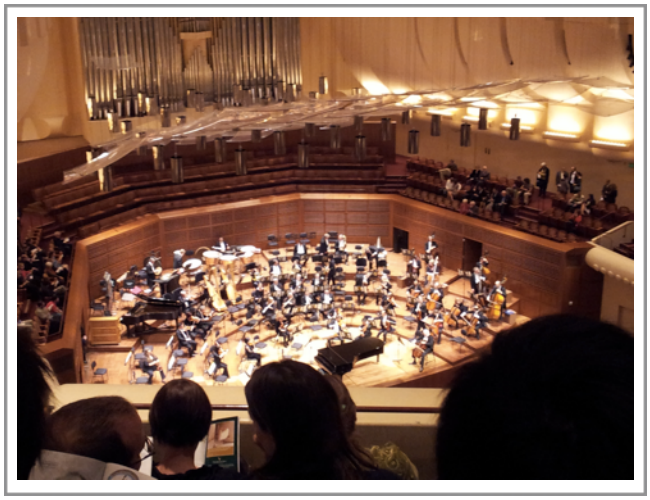
거기있는 내내 내게 영어는 늘 고민거리여서 시에서 운영하는 Berkeley Adult School 에서 무료 English as Second Language 강의를 들었다. 무료임에도 불구하고 수업의 질은 나쁘지 않았다. 반에는 여러 나라에서 모인 사람들이 있어서, 사람들과 이야기해보는 것도 즐거움 중 하나였다(수강생들의 국적은 총 20개국이 넘었다). 선생님은 외향적인 사람들 뿐 아니라 내향적인 사람들도 말할 기회를 갖을 수 있게 배려해준다. 사람들과 팀을 이뤄 무언가를 하는 과정에서 다른사람들과 얘기도 많이 나눌 수 있다. 나중엔 같은 국적의 사람들이 팀을 이뤄 모국을 소개하는 프레젠테이션을 했는데, 나는 그 전에 귀국하느라 참여못한게 아쉽

다. 혹시 나중에 버클리를 방문하는 사람들은 Berkeley Adult School 의 ESL 수업에 참여하는 것을 고려해보길 권한다.

덧붙여 나처럼 영어로 어려움을 겪는 분들에게 무조건 크게말하면 통할 가능성이 조금이라도 높아진다는 것을 말하고 싶다. 영범이 형이 mit방문기에서 언급했듯이, 영어가 통하기 위해서 제일 중요한 것은 문법도 풍부한 어휘도 아닌 발음이었는데, 발음은 모두가 알다시피 억양과 강세를 잘 알아야한다. 그런데 서투른 억양과 강세로도 크게 또박또박 말을 하면 사람들이 알아들을 확률이 높아지는 것을 알게되었다. 그러고보니 사람들이 영어를 자신감 있게 말하라고 강조하는 이유가 있었다. 낮은 영어실력에 자신감 갖기 어려운게 사실이었지만, 한번 용기를 내 자신감 있게 크게 말하면 선순환이 시작되는 것 같다.

여가 활동

음악



버클리에는 생음악을 겸한 바, 카페, 레스토랑이 심심찮게 있어서 음악을 접할 기회가 많았다. 음악을 접하러 샌프란시스코로 나가기도 했는데, Yoshi's 라는 공연장 겸 레스토랑에서 재즈 공연을 관람하기도 했고 Davis Symphony Hall 에서 좋은 클래식 공연을 관람하기도 했다. 버클리 캠퍼스 내에서도 무료 혹은 유료의 클래식, 오페라 공연이 열렸다. 음악을 접하기 좋은 환경이었다.

관광

가끔은 주말을 틈타 샌프란시스코, LA, 라스베가스로 도시 관광을 가기도 했다. 샌프란시스코에서 인상깊었던 것은 매년 11월 초 경에 열리는 멕시칸 할로윈데이 축제(El Dia De Los Muertos)였는데 사람들이 죽은 사람을 연상시키는 다양한 화장과 의상으로 자기를 꾸미고 거리에서 춤을 추거나 서로 사진을 찍는다. 원래 멕시칸들의 축제라서 그런지 아즈텍 전사들로 꾸민 사람들의 퍼레이드도 볼 수 있었다.

라스베가스에서 가장 인상깊었던 것은 르레브라는 서커스 공연인데 화려한 조명과 무대

장치들, 기예, 군무들이 버무려진 공연이다. 라스베가스에 간다면 관람을 강추한다.

다국적 팀

드로이드 블레이즈 팀은 미국인 2명, 인도인 1명, 한국인 3명, 중국인 5명, 이탈리아인 1명으로 구성되어있다. 한국인은 희종, 원찬이형과 나인데, 희종이형은 내가 오기 전에 귀국하여 한국에서 원격으로 일하고 있었고, 원찬이형은 나와 한달여를 함께 일하다가 한국으로 돌아가서 마찬가지로 원격으로 일했다.

같이 일한 인도인 Vijay D'Silva 는 인격적으로나 실력적으로나 완벽한 사람인 것 같다. 내게도 여러모로 도움을 줬다. 영어 때문에 소통에 문제가 생기면 도와주기도 하고, 자신의 연구내용이나 흥미로운 아이디어/논문들의 내용을 개인교습해주기도 하였다. Vijay 에 대한 고마움은 잊지 못할 것이다.

그리고 동적 분석을 하는 중국인 3명(hui, xiaoyin, shuaifu)과도 친하게 지내고 지내면서 도움도 많이 받았다. 이탈리아인 alessandro 는 이탈리아인 답게 장난꾸러기인데 자기 옆자리에 중국인 hui 의 컴퓨터를 해킹해서 hui가 한창 일하고 있는 도중 포르노 사이트를 팝업시키기도 했다. 그 후 벌어진 hui 와 alessandro 의 보안배틀은 아직도 기억에 남는다. 팀원들이 하나같이 다들 개성있고 착해서 이들과 같이 일한 경험은 오래간 좋은 기억으로 남을 것 같다.

거주 환경

나는 UC village 라는 버클리 대학교 차원에서 가족이 있는 학생들을 위해 만든 거주지역에서 지냈다. 이곳엔 한국인들이 많이 살았다. 한달은 이미 버클리에서 유학하고 있는 원태형 집에서, 나머지 기간은 원태형 집 바로 위층에서 한국인 유학생 둘과 함께 지냈다.

결과적으로 한국인들이 사는 곳에 함께 살아서 가장 좋았던 것은 위급상황이 발생했을 때였다. 어느 날 자전거 타고 집으로 돌아오는 길에 혼자 넘어지는 바람에 팔꿈치 뼈에 금이 갔는데, 원태 형과 룸메이트, 빌리지에 사는 다른 한국인 유학생 형이 내가 응급실에서 진료받을 수 있게 도와주었다. 미국은 앰뷸런스를 부르기만해도 수백만원이 청구되기 때문에, 만약 차도 없는 내가 근처에 도움 요청할 곳 없는 원룸에서 혼자 살았더라면 더 큰 곤경에 처했을 것이다.

사고들

미국은 안전망이 잘 갖춰진 나라는 아니란 생각이 든다. 나는 지내는 동안 자전거도둑과 자전거사고를 당했고, 직접 당하진 않았지만 학교 근처에서는 총기강도가, 버클리에서 멀지 않은 오클랜드에서는 총기 살인사건이 일어나기도 했다.

자전거 사고는 미국 의료보험의 실태를 체감할 수 있는 경험이었다. 나는 팔꿈치 뼈에 금이가서 응급실에서 엑스레이를 찍고, 깁스 감고, 파상풍 주사를 맞았다. 아직 응급실 비용이 청구되지 않아 금액을 알 수 없는 상태지만, 적어도 100만원 내외가 청구될 것이라는 것이 미국생활을 오래한 내 룸메이트들의 예상이다. 물론 의료보험이 있으면 지출이 줄어들지만 내가 구입한 의료보험은 최소한의 보장만 되는 catastrophe-only 보험이었기 때문에 3천달러를 초과하지 않는 모든 의료비는 전액 내가 부담해야한다. 응급실 진료 후 정형외과 의사를 만나려고 약속을 잡기도 했는데, 의사 얼굴을 보는 것만으로 청구될 예상금액을 듣고 약속을 취소하기도 했다. 더 큰 경제적 출혈을 막기 위해서(그리고 오른팔을 못써서 일을 못하기도 해서) 사고 후 급히 귀국했는데 결과적으로 예정보다 보름정도 일찍 귀국한 셈이다.

자전거 도둑질을 당한 경험도 황당했다. 자전거를 주차금지 표지판에 묶었는데 누군가 주차금지 표지판을 떼고 자전거를 기둥위로 들어올려서 가져갔다. 표지판 기둥의 높이가 꽤 높았기 때문에 미처 상상도 못했던 방법에 허를 찔렸다. 미국은 자전거가 다 비싸기 때문에 이 또한 출혈이 컸다.

미국을 방문할 분들은 국내보험이든 미국보험이든 보장사항을 꼼꼼히 잘 체크하여 준비하고 응급상황시 연락할 사람을 잘 알아두어야한다. 또한 자전거를 탈 때는 안전장비를 꼭 잘 갖추고 타고 안전한 곳에 묶어야 한다.

마치며

짧지도 길지도 않은 미국생활을 통해서 세상 보는 시야를 많이 넓힐 수 있었다. 좋은 경험을 할 수 있게 허락해주신 이광근교수님께 감사드린다. 그리고 지내는동안 수 많은 도움을 준 원태 형과 Vijay 에게도 감사드린다.