<picture from https://www.flickr.com/photos/gary_leavens/45081113374/>

FSE'18 Trip Report

Florida, USA

2018.11.5 ~ 2018.11.9

고려대학교 소프트웨어 분석 연구실

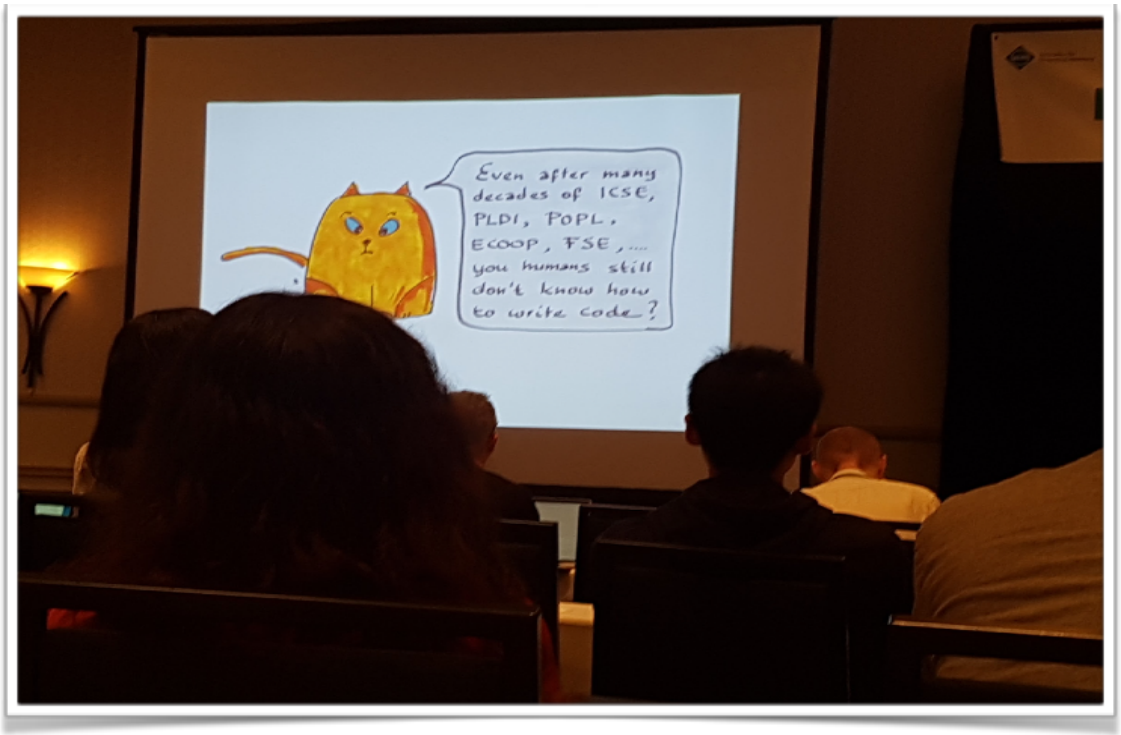
홍성준

1. 개요

FSE는 ICSE와 더불어 소프트웨어 공학 분야에서 가장 유명한 학회 중 하나이다. 메모리 해제 오류 자동 패치에 관한 논문이 채택되어서 저자로서 참가하게 되었다. 올해 FSE는 플로리다 디즈니 스프링스 리조트에 위치한 호텔에서 열렸는데, 디즈니 컨셉의 호텔이라 뭔가 특이한 것이 있나 싶었으나 별다른 것은 없었고 그냥 학회였다. 메인 컨퍼런스 앞 뒤로 Doctorial symposium, automated specification inference에 관한 워크샵인 WASPI 등이 열렸고, 총 참가자는 400명이 조금 안되는 숫자였다. 매우 큰 규모로 열리는 ICSE만 참가해봐서 그런지는 몰라도 학회 규모가 굉장히 작다는 느낌이 들었다. 덕분에 학회 내내 마주쳤던 사람을 계속 마주칠 수 있어서 말을 붙이거나 교류를 하기에는 더 수월했다.

2. 학회 전반

• 키노트



메인 컨퍼런스의 매일 아침은 키노트로 시작했다. 이 중에서 첫 날 Facebook의 Erik Meijer가 발표한 톡이 제일 기억에 남았다. 큰 주제는 소프트웨어 2.0에 관한 내용이고, 그 중에서도 딥러닝 프레임워크의 군데군데는 PL 분야에서 제안된 여러 concept이 녹아있다는 내용이었다. 사실 그 연결고리는 제대로 이해하지 못했으나 소프트웨어 2.0 이라는 새로운 패러다임을 설득시키는 방식이 재미있었다. 아직은 사람들(적어도 나를 포함해서)이 데이터에 의해 프로그램이 작성되는 방식이 과연 믿을만 한가에 대해 의문을 갖고 있다. 위 슬라이드의 포인트는, 사람들이 ICSE, PLDI, POPL 등의 유수 학회에서 수십년동안 프로그래밍에 대한 끈질긴 고민을 해왔음에도 여전히 제대

로 코드를 작성하는 방법에 대해 완벽히 이해하지 못하고 있다는 것이다. 너도 안되는 걸 나한테 묻지말라는 식의 논리이긴 하지만, 소프트웨어 1.0 패러다임에서의 프로그램은 신뢰하면서 2.0 패러다임은 받아들일 수 없다는 사람들에게는 좋은 반박 포인트 인 것 같다. 또 기억에 남는 것은 모든 슬라이드가 만화체로 되어있었다는 것이다. 전문가 수준의 그림실력에 말도 잘해서 발표 내내 지루하지가 않았다. 발표를 잘 할 수 있다면 관중을 집중시킬 수 있는 매우 효과적인 방법인 것 같다.

• 학회 점심

<picture from https://www.flickr.com/photos/gary_leavens/45081113374/>

음식의 질은 꽤 만족스러웠다. 외주 뷔페식은 아니었고, 학회 호텔 내의 디즈니 레스토랑을 통째로 빌려서 해당 레스토랑의 요리가 제공되었다. 이번에는 일행이 준희 형 뿐이라 매일 새로운 테이블에서 모르는 사람과 점심을 먹었고, 개인적으로 신선한 경험이었다. 밥먹기 전에 자기소개 한 두마디와 무슨 연구를 하는지 등을 설명할 기회가 있었지만, 식사 도중 대화가 무르익으면 거의 끼어들 수가 없었다. 영어에 대한 부족함은 항상 느끼지만 학회를 가면 특히 더 절실하게 깨닫는 것 같다. 특히 SE에서 생소한 분야에 대한 대화가 시작되면 무슨 말을 하고 있는지 이해하기도 버거웠다.

• 교류

일행이 적어서인지 확실히 지난 학회들보다는 처음보는 사람들과 교류할 기회가 많았다. 특히 첫 날 커피 브레이크에서 Yui Le가 나를 먼저 알아봐주어서 반가웠다. 그는 Tian Tan과 포인터 분석 연구를 하는데, SE 학회는 처음와본다고 했다. 또 기억에 남는 사람들로는 Eric Bodden 연구실의 학생과 TU Darmstadt 소속의 학생이 있었다. 각각 현존하는 taint analyzer들에 대한 평가, 디버거 디버깅 연구에 관한 발표를 했다. 또 우연찮게 홍콩과기대 김성훈 교수님 연구실의 한국인 박사과정 분을 만났는데 유닛 테스팅에서의 precision에 관한 연구를 하는 분이었다.

특히 이번에는 구글 deep static analysis 팀의 수장인 Omer Tripp과 점심을 먹을 기회가 있었다. Facebook의 경우에는 Infer 분석기를 접점으로 어떤 프로젝트를 진행하고 있는지 대략 알고 있었지만 구글의 정적 분석 팀에서는 무슨 일을 하고 있는지 잘 알지 못했던 터라, 나에게도 유익한 시간이었다. 우리의 논문에 대해 좀 더 자세히 설명해주고, 나도 구글 팀에서는 어떤 분석을 하는지 구체적으로 물어보았다. 우리 기술에 대한 질문은 정적 분석에 관한 내용부터 구현 디테일까지 물어보았는데, 아마 바쁘셔서 그런지 논문 디테일은 안읽어본 것 같았다. 어떻게 반드시 객체를 해제하는 해제문을 찾는지, 분석기 엔진은 어떻게 구현했는지, 어떤 벤치마크로 평가했는지 등에 대해 물어보았다. 우리 그룹에서 진행중인 다른 프로젝트에 대해서도 설명해주었는데, 모두 흥미로워 했다.

3. 논문 발표

MemFix: Static Analysis-Based Repair of Memory Deallocation Errors for C
이준희, 홍성준, 오학주

이 논문은 정적 분석을 사용해서 프로그램에 각 객체(allocation-site)에 대해 메모리 해제 오류가 없도록 하는 해제문의 조합을 찾아주는 기술을 제안한다. 입력으로 메모리 해제 오류가 존재하는 프로그램이 들어왔다면, 해당 객체의 오류가 없을 조건을 만족하는 해제문의 조합을 찾아줌으로써 오류를 자동으로 고치는 식이다. 기존의 자동 패치 논문들과 가장 큰 차별점은 생성된 패치는 새로운 오류를 일으키지 않으며 기존의 오류를 반드시 고친다는 점이다. 두 포인트는 프로그램 자동 수정 기술의 대세라고 할 수 있는 테스트케이스 기반의 패치 생성 기술들 대부분의 근본적인 한계이다. 실제로 연구를 시작할 때 주된 동기는, 프로그램이 기껏 1~2 줄씩 수정되는데 여러명의 개발자가 해당 코드를 다시 리뷰하고 있다는 불편함에서 출발한 것이었다. 발표에서도 이 점을 동기로서 전달하려고 노력했다.

발표는 공동저자인 준희형이 했다. 발표 준비는 꼬박 한 달이 걸렸고, 출국 이틀 전까지도 슬라이드가 완성이 안될 정도로 많은 수정이 있었다. 많이 고민한만큼 최종 슬라이드 퀄리티는 개인적으로 만족스러운 수준이었다. 발표에서 주로 전달하려고 했던 내용은 리뷰가 필요 없는 패치를 만들어야 하는 이유, 그러한 패치를 만들기 위해서 패치 문제를 Exact Cover Problem으로 표현하는 아이디어와 이를 위한 정적분석의 디자인이었다. 실제 발표는 꽤 잘했다고 느껴졌다. 목소리도 커서 무슨 말을 하는지 잘 들렸고 우리가 준비했던 얘기를 모두 다 할 수 있었다. 발표 직후의 질문은 여러 개가 나왔는데 그중에는 알아들었으나 매끄럽게 대답하지 못한 것도 있고, 질문 자체가 이해가 안가는 것도 있었다. 하지만 질문자들 모두 결국은 납득을 했던 것 같다. 주로 나왔던 질문은

- Scalability에 대해 어떻게 생각하고 이를 어떻게 해결할 계획인가?
- Review가 필요없는 패치를 생성한다고 했는데, 실제로 개발자들이 납득할 수 있다고 생각하냐

등 이 있었고, 세션 체어, 질문자, 일부 청중들이 서로 대답을 해주기도 하고 새로운 의견을 내놓기도 했다. 예를 들면 Coreutils정도라면 크기는 작지만 충분히 real-world program이고, verified patch와 scalability는 trade-off가 있을 수 밖에 없지 않느냐는 변호를 해주는 사람이 있었는데 매우 고마웠다. 또, 리뷰가 필요없는 패치라고 하더라도, 개발자에게 분석 결과를 visualize해서 패치를 생성한 근거로서 제공하면 좋을 것 같다는 의견도 있었다.

세션이 끝나고도 개인적으로 질문을 하러 오는 사람이 여러명 있었다. 실제로 고칠 수 있는 프로그램인데 해를 못 찾는 경우가 있을 수 있는지에 대해 설명해달라는 질문, 우리의 툴이 오류 탐지까지 같이하는지, 만약 오류가 없는 프로그램이 들어오면 어떻게 되는지에 관한 질문 등이 있었다. 사실 두 번째 질문은 발표만 들어서는 충분히 궁금할 수 있는 사항이였는데 잘 대답해주지 못한 것 같아서 아쉬웠다.

결과적으로 잘 마무리 된 발표였다. 실제 툴의 유용성과 scalability등에 관한 질문이 가장 걱정이었는데, 아이디어 자체를 좋아하는 사람도 생각보다 많았고, 학회에서 남의 연구에 대해 작정하고 칼같이 비판하려는 연구자는 생각만큼 없다는 것을 새삼 깨달았다.

4. 인상깊은 발표들

Syntax-Guided Synthesis of Datalog Programs
Xujie Si, Woosuk Lee, Richard Zhang, Aws Albarghouthi, Paris Koutris, Mayur - Naik

입/출력 예제로부터 Datalog 프로그램을 자동으로 합성하는 기술에 관한 논문이다. Xujie Si라는 저자가 발표했는데, Datalog와 프로그램 합성 모두 친숙한 주제임을 감안하더라도 FSE에서 내가 들은 톡중에 가장 잘한 발표였다. 기존의 제안된 합성 기술들은 각각 유저로부터 프로그램 템플릿을 입력으로 받거나, 매우 많은 수의 입/출력 예제를 요구하거나, 2~3 개의 룰로 이루어진 간단한 프로그램만을 합성할 수 있는 한계가 존재한다. 이 연구에서는 각각의 한계를 정의하고 이를 해결하기 위해 어떤 아이디어를 사용했는지가 굉장히 명확하게 드러났다. 특히 눈여겨볼 점은 각 한계를 해결하기 위한 어프로치가 휴리스틱하지만 (내 생각에) 굉장히 합리적으로 느껴져서 별로 단점처럼 보이지가 않았다는 것이다. 예를 들어, 템플릿의 경우 여러 저자들이 Datalog 프로그램에 자주 등장하는 패턴을 관찰한 결과를 바탕으로, 해당 패턴을 systematic하게 생성해내는 어프로치이다. Main challenge라고 할 수 있는 탐색 공간을 효율적으로 탐색하는 문제 역시 고전적인 휴리스틱인 Query-by-Committe라는 컨셉으로 해결했다. 현재 내가 진행하고 있는 SAVER 프로젝트도 비슷한 방식으로 presentation하면 충분히 잘 설명할 수 있겠다는 생각을 했다.

Symbolic Execution with Existential Second-Order Constraints
Sergey Mechtaev, Alberto Griggio, Alessandro Cimatti, Abhik Roychoudhury

이 논문은 전통적인 first-order symbolic execution에 existential second-order constraint 가 확장된 새로운 기술을(SE-ESOC)을 제안한다. 그리고 프로그램 자동 패치와 library function의 spec을 추론하는 application을 통해 기술이 유용함을 보였다. SE-ESOC은 프로그램의 함수를 symbolic function variable로 치환하고 그 interpretation을 합성해낸다. 예를 들어, array에서 predicate 을 만족하는 index를 찾는 `search(data, pred)`함수에서, 입력 배열 `[0, 1, 2]`에 대해 함수가 2를 반환하게 하는 predicate이 무엇인지를 찾는 상황이라면, SE-ESOC은 `search([0, 1, 2], ρ)`을 실행하여 `ρ := λx. x > 1`와 같은 해를 합성해낸다. Application domain이 기본적으로 first-order theory를 적극 활용하는 만큼, 이 연구에서는 second-order formula solving에 특화된 solver 대신에 기존의 first-order solver의 강점을 같이 활용할 수 있는 approach를 택했다. 이를 위해 formula를 first-order로 인코딩하기 위한 효율적인 테크닉을 제안했다.

저자인 Sergey Mechtaev는 주로 symbolic execution을 이용해서 semantic program repair를 생성하는 연구를 한다. 작년 ICSE에서도 reference implemenation을 활용하여 패치를 생성하는 연구에 대한 발표를 들었던 기억이 있다. Symbolic execution을 도구로 사용하던 연구를 계속 하다가 더 나아가 이를 개선 하는 경지에 까지 이른 것 같다. 자동 패치 생성 분야에서 굉장히 잘 하는 사람 같아서 눈여겨 보고 있었는데, 개인적인 이유로 이번 학회는 참석하지 못했다고 해서 아쉬웠다.

5. 여행기

플로리다 날씨는 따뜻한 정도가 아니고 우리나라 한여름 날씨만큼 덥고 습한 날씨였다. 학회가 열린 Lake Buena Vista 지역은 예전에 ICSE를 다녀오면서 묵었던 마이애미만큼 북적대는 휴양지 느낌은 아니였고, 디즈니 테마파크가 있어서 유명한 정도인 것 같았다. 우리는 학회 시작 전날인 월요일에 도착했는데, 호텔에 들어가자마자 피곤해서 잠을 자는 바람에 밤이되어 돌아다니지 못했다. 저녁 시간도 지나버려서 전화로 도미노 피자를 시켰다. 영어로 전화로 피자 주문을 하는 것은 처음이라 만반의 준비를 했다. 결국 주문한 것과는 조금 다른 피자가 왔지만 배가고파서 그런지 아주 맛있었다.

이 지역의 랜드마크는 유니버셜 스튜디오, 씨월드, 디즈니 테마파크 정도인데, 모두 놀이공원정도로 생각하면 된다. 날잡고 아침일찍 출발해야 제대로 즐길 수 있는 컨텐츠라서, 학회가 끝난 다음 귀국하는 당일밖에 시간이 나지 않았다. 결국 마지막 날 호텔 근처에 디즈니 스프링스 리조트를 가기로 했다. 디즈니 스프링스 리조트는 입장료를 받는 테마파크는 아니고 디즈니 기념품을 파는 굉장히 거대한 쇼핑지구라고 생각하면 된다. 화창한 날씨 덕분인지 나름 만족스러웠다.

6. 마치며

처음부터 끝까지 준희 형과 같이 진행한 연구였는데, 서로 성향이 달라서 결과적으로 좋은 조합이었다는 생각이 든다. 또, 분석기 디자인 및 구현까지 직접 해볼 수 있는 좋은 경험이었다. 논문 제출 당일날 목구멍으로 잘 안넘어가던 피자, 제출을 하고도 이것저것 할게 많아서 고생했던 기억이 아직도 생생하다. 끝으로, 항상 좋은 연구를 지속할 수 있도록 격려해주시고 아낌없이 지원해주시는 오학주 교수님께 진심으로 감사하다는 말씀을 드리고 싶다.