Srini Devadas

Capsule Introduction

SNU CSE Distinguished Lecture Series

Srini Devadas 는 MIT Electrical Engineering and Computer Science (EECS) Department 의 Edwin Sibley Webster 석좌교수이며, CSAIL (Computer Science and Artificial Intelligence Lab) 소속의 PI 이다. Devadas 교수는 반도체 칩 설계를 위한 CAD (Computer Aided Design)부터 컴퓨터 아키텍처 및 시스템, 컴퓨터 보안, 계산 생물학(Computational Biology), 암호학에 이르기까지 폭넓은 분야에서 탁월한 연구 성과를 거두었다.

특히 그는 보안 프로세서 분야에서 선구적인 업적을 남겼다. 2003-2005 년에 개발한 Aegis 는 운영체제를 신뢰하지 않는 싱글 칩 보안 프로세서로, 이후 Intel 의 Security Extension 인 SGX 에 채택된 여러 보안 개념을 최초로 제시하였다. 2016 년에는 Intel SGX 의 상세한 분석을 바탕으로 SGX 보다 향상된 보안을 제공하는 오픈소스 RISC-V CPU 인 Sanctum 을 설계하였다.

또한, Devadas 교수는 실리콘 기반의 Physical Uncloneable Function (PUF)을 세계 최초로 개발한 것으로 잘 알려져 있다. PUF 는 칩 제조 과정의 물리적인 변동성(process variation)을 이용한 신개념의 비밀 키(secret key) 생성 기술이다. 이 기술은 Xilinx, Altera 의 FPGA 와 Samsung 의 Galaxy Note 제품군에 채택된 Exynos 프로세서 등 다양한 상용 제품에 적용되었다.

Devadas 교수는 MIT 에서도 인정받는 천재형 학자이다. 그는 1985 년 IIT Madras 에서 학사학위를 취득하고, 이듬해 UC Berkeley 에 석박통합과정으로 진학하여 3 년 만에 박사학위를 수여 받았다. 그리고 만 24 세의 나이로 MIT EECS 에 조교수로 부임하였다. 이는 2001 년 알고리즘을 전공한 Erik Demaine 교수가 20 세의 나이로 조교수로 부임할 때까지 최연소 기록으로 알려져 있다.

나는 MIT 에 진학한 후 첫 지도교수로 Devadas 교수와 3 년간 함께 일했는데, 그때 PUF 의 첫 프로토타입 칩을 설계했고, 훗날 Dynamic Information Flow Tracking (DIFT)으로 알려진 보안 프로세서 연구를 함께 하였다. 당시에는 그 연구의 의미를 완전히 이해하지 못했지만, 이후 컴퓨팅 환경에서 대규모 보안 이슈가 불거지면서 시대를 앞서간 매우 영향력 있는 연구가 되었다. (여담으로 PUF 논문은 2017 년에 IEEE VLSI Symposium 에서, DIFT 논문은 2014 년에 ACM ASPLOS 에서 모두 test-of-time award 를 수상하는 기쁨을 그와 함께 누렸다.)

이후 보안 연구를 더 추구하고자 하는 Devadas 교수와 정통 아키텍처 연구를 하고 싶었던 나의 생각 차이로, 나는 결국 다른 지도교수(Krste Asanovic, RISC-V 아키텍처 창시자)의 지도로 박사학위를 받게 되었다. 그렇지만, 처음 연구를 그와 함께 하면서 알게 모르게 연구 스타일에 그로부터 많은 영향을 받았다. 특히, 좋게 말하면 폭넓고, 나쁘게 말하면 다소 산만한 나의 연구 주제는 분명히 그의 영향이라고 생각한다.

지난 2023 년 여름에 MIT 를 방문했을 때, 거의 10 년 만에 만났음에도 간단한 수인사 후에 자신이 최근 생각한 연구 아이디어를 화이트보드에 한 시간 동안 펼쳐놓는 그를 보며, 천상 학자가 이런 분인가 싶었다. 앞으로도 더욱 왕성한 연구 활동으로 학계와 산업계에 기여하시기를 기원한다.

이재욱, 2024 년 8 월