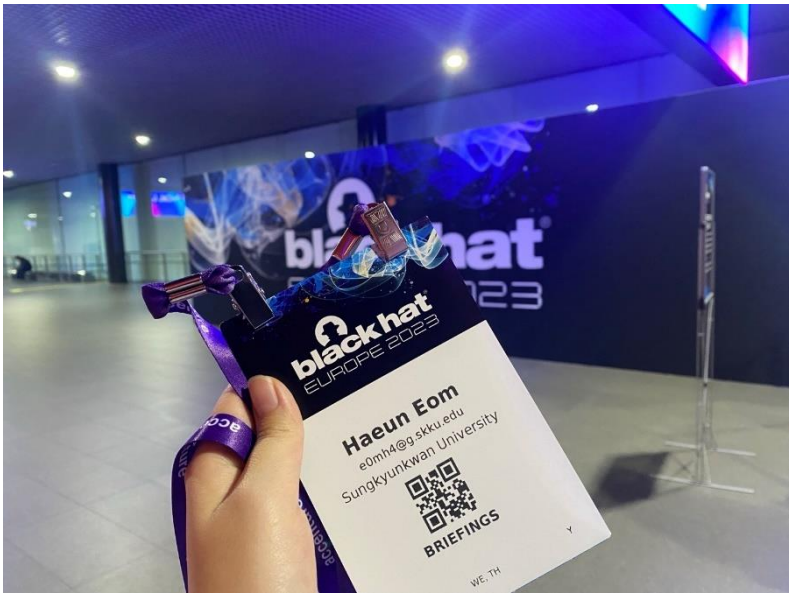
Black Hat Europe 2023

Trip Report

London, United Kingdom

Haeun Eom



1. 개요

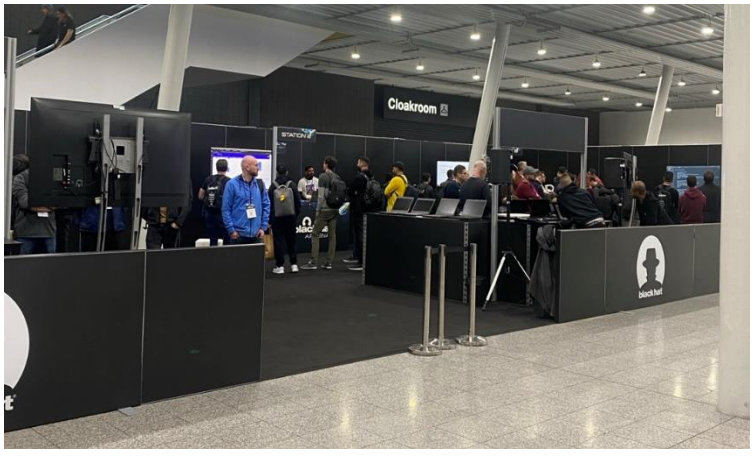
컴퓨터 보안 분야에서 유명한 해킹 컨퍼런스인 블랙햇 유럽(Black Hat Europe)에 참석하였다. 대학원 진학 후 처음 참석한 해외 컨퍼런스로, 해킹에 대한 기술적인 지식도 많이 없고 영어도 잘 하지 못해 대부분의 발표를 자세히 이해하진 못하였다. 하지만 온라인으로는 알 수 없는 현장에서의 분위기와 해커들의 네트워킹을 보고, 다음에는 저 사이에서 발표자로 내 경험을 얘기하면 좋겠다는 생각에, 언어와 기술적 배경지식을 향상시키기 위해 열심히 공부하겠다는 큰 동기를 얻었다. 본 리포트에서 이번 학회와 여행에서 경험한 것을 위주로 공유하고자 한다.

2. Black Hat Europe 2023 참석

2.1 컨퍼런스 분위기

블랙햇 컨퍼런스는 학회 느낌보다는 해커들의 네트워킹 파티 같았다. 해외 학회에 참석해보진 않았지만, 국내 학회와 운영은 비슷하게 된다고 들었었다. 아직 경험이 많지 않아서 그런지 몰라도 학회는 살짝 각진 느낌으로 논문 발표를 위한 공간 같다면, 블랙햇은 '나 이런 연구 했어. 관심있으면 나 따라와. 얘기 나누자' 이런 느낌이었다. 세션 별로 모두 조명이 화려하게 달려있어서 그런지 편하게 강연을 보는 것 같았다.

또한, 유명한 해킹 컨퍼런스여서 그런지 굿즈샵도 있었고, job fair처럼 회사 소개하는 부스들도 있었다. CES에 참석해 본 적이 있는데, CES와 느낌이 비슷했다. CES에서 새로운 제품을 발표하고 각 회사별로 제품을 소개하는 것처럼, 블랙햇에서는 새로운 취약점을 발표하고 각 회사별로 어떤 일을 하는지 소개하는 분위기였다.



2.2 발표

블랙햇 유럽은 동시에 4개의 세션에서 1개의 발표가 진행되었다. AI, Mobile, Hardware/Embedded, Application security, Cloud 등 다양한 타겟에 대해 취약점을 찾은 경험에 대한 발표가 열렸다. 해킹 컨퍼런스이다 보니 타겟, 방법 전부 다양해서 대부분 처음 들어보는 것이었다. 당장 이해한 내용은 다소 부족하긴 하지만 발표자들이 분석한 내용을 기반으로 추후에 비슷한 타겟을 분석할 때 도움이 될 것 같았다.

동시에 여러 세션이 진행되어서 앞 내용을 모르는 상태로 뒤의 얘기를 들으면 더욱 이해하는데 어려울 것 같아, 한 번에 하나의 발표만 들었다. 그 중 흥미로웠던 발표를 소개한다.

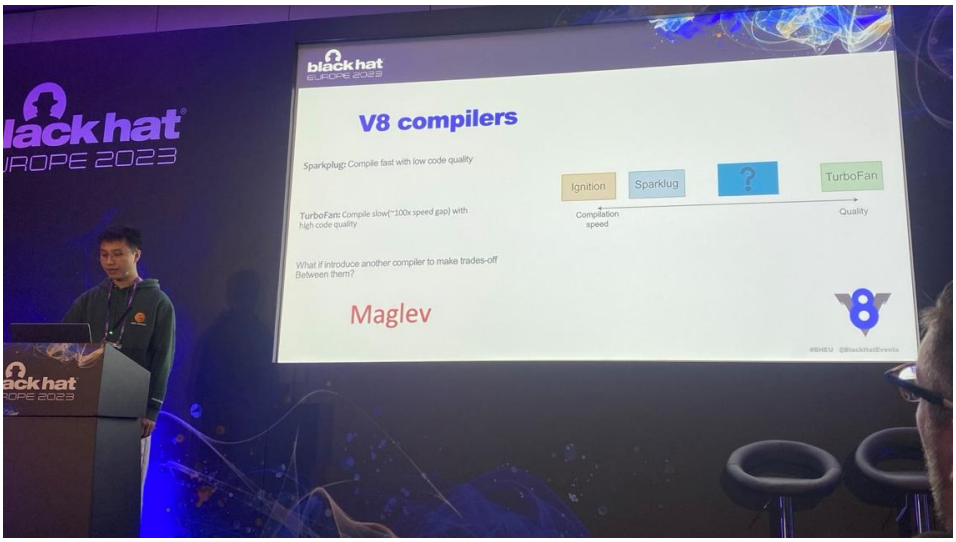
Reviving JIT Vulnerabilities: Unleashing the Power of Maglev Compiler Bugs on Chrome Browser

본 발표는 mid-tier JIT Compiler인 Maglev Compiler의 Attack surface와 발견한 취약점에 대해 소개하고 있다. 발표자들은 JIT Compiler가 보안에 취약하고, V8의 기존 최적화 컴파일러 중 하나인 Turbofan의 bug mitigation이 견고해지면서, 2022년부터 활발하게 개발되기 시작한 Maglev Compiler가 Turbofan과 비슷한 구조를 가지고 있어, Maglev Compiler를 대상으로 취약점 분석을 시작하였다. 발표자들이 Maglev를 Turbofan과 비교한 결과, Register Allocation, Inline, Deoptimization 측면에서는 Turbofan과 유사하지만, Phi untag, Special deoptimization design, Special Structure like Try-catch、Loop related

issue와 같은 Maglev만의 attack surface도 존재한다는 것을 확인하였다. 식별한 attack surface를 대상으로 효율적인 취약점 발견을 위해 Crash-based Fuzzer, Differential Fuzzer, CodeQL을 활용하였다고 한다. Fuzzer와 CodeQL을 활용하여, 7개 취약점을 찾았고, 그 중 하나의 취약점으로 RCE까지 성공하였다고 한다.

본 발표를 들으면서 기존 연구 동향의 중요성을 다시 한번 확인할 수 있었다. 발표자들은 Maglev와 비슷한 기능의 컴파일러인 Turbofan을 확인하였고, Turbofan의 1-day와 구조들을 확인하여 Maglev에 대한 이해도를 높였다. 기존의 분석들을 활용함으로써, 분석 및 이해의 시간을 줄일 뿐만 아니라, 기존의 attack surface들은 어떤 것이 있었고, 해당 surface에서는 어떤 공격들이 이루어졌는지 등을 확인해 비슷한 취약점이 내 타겟에는 없는지 볼 수 있다. 본 발표자들은 이런 부분을 제대로 활용한 것 같다. 발표에서도 Maglev의 버그와 비슷한 버그 유형들이 다른 JIT compiler에도 존재하는 것을 보여주었다. 기술적인 부분들은 아직 이해하진 못했지만, 방법론적인 부분에서는 기존 연구 분석, 기존 기술을 내 타겟에 어떻게 응용하는지 알 수 있는 발표였다.

그리고 좀 발표 외적인 얘기이긴 하지만 본 연구진들은 중국인으로 나는 한국식 영어를 주로 들었어서 그런지 영어 발음을 이해하기 어려웠다. 주변 외국인들을 봤을 때, 다들 이해하지 못한 표정이었다(내가 이해를 못해서, 다른 사람도 그랬을 것이다 생각했을 수도 있다). 발표장에서 발표자들은 영어에 대한 부담감도 없어 보였고, 본인의 연구를 발표하는 것이어서 그런지 자신감 넘쳐 보였다. 이런 태도도 배울만한 부분이었다.



Old Code Dies Hard: Finding New Vulnerabilities in Old Third-Party Software Components and the Importance of Having SBoM for IoT/OT Devices

본 발표는 IoT장비들이 펌웨어 파일 암호화 같은 security by obscurity와 open source

components를 선택할 때 공개된 CVE가 없으면 안전할 것이라는 principle of many eyes에 의존하고 있는 점을 지적하고 있다. 이런 원칙이 공격자에게는 도움이 된다는 점을 보여주기 위해, IoT 네트워크의 엣지에서 흔히 볼 수 있는 Sierra Wireless AirLink 게이트웨이를 분석하였다. 해당 장비에서의 기존 취약점은 어느 것도 펌웨어에서 동작하는 오픈 소스에 대해 보지 않았다고 한다. 그래서 발표자들은 장비에서 펌웨어를 추출하고, rp-pppoe, OpenNDS, TinyXML, libmicrohttpd에 집중해 취약점 분석을 진행하였다. 총 21개의 취약점을 찾았는데 15개가 open-source component에서 발견되었다고 한다. 하나만 자세히 얘기하자면, TinyXML의 경우, TinyXML2로 대체되어 이젠 지원되지 않는데,

TinyXML을 사용하고 있었고, TinyXML 코드로 libFuzzer를 사용해 간단히 Fuzzer를 만들어 돌린 결과 몇 초 만에 취약점을 찾을 수 있었다고 한다.

이 발표 내용은 내 연구에도 직접 적용해볼 수 있을 것 같아서 흥미로웠다. 지금 하고 있는 연구에서도 서비스에 GStreamer라는 open-source 프레임워크를 사용하고 있는 것으로 확인하였는데, 기존 GStreamer의 취약점이 내 연구대상에도 적용가능한지 확인해보는 것도 좋을 것 같다. 이 외에도 starlink는 라우터에서 openWRT를 사용하고 있어서 여러 장비에도 적용해볼 수 있지 않을까 생각이 들었다. 또한, 살짝 다른 범위일수도 있지만 버전 별 취약점들도 확인해보면 좋지 않을까 생각이 들었다. 예전에 steam을 분석할 때 v8 engine의 버전이 낮은 버전으로 작동하고 있었어서, 이런 부분에서도 기존 취약점을 활용할 수 있지 않을까 생각이 들었다.

HODOR: Reducing Attack Surface on Node.js via System Call Limitation

본 발표는 node.js에 attack surface를 줄이기 위해 HODOR이라는 기법을 제안하고 있다. 내가 들은 발표들 중에서는 가장 학술적인 느낌이었다. 발표 흐름은 기존 node.js의 취약점과 이를 해결한 기존 방식들을 얘기하고, 기존의 challenge를 해결한 본인들의 기법을 제안하고 있다. node.js의 npm 패키지의 20%가 ACE attacks으로 이어질 수 있어서, ACE attack surface를 줄이기 위해 기존에는 프로그램 분석을 통해 useless code를 지우거나

(RAZOR-usenix'19, Mininode-RAID'20) 어플리케이션에서 사용할 수 있는 시스템콜을 제한하는 방식(sysfilter-RAID'20, Saphire-usenix'21)을 이용했다고 한다. 하지만 여전히 cross-language mapping이 필요하고, Node.js 프레임워크 integration문제가 있다고 한다. 그래서 본 연구는 애플리케이션의 정상적인 실행에 영향을 주지 않으면서 시스템 호출 수준에서 공격 표면을 최소화하는 기법을 제안하였다. Call graph를 이용해 Built-in Module layer에 대한 LLVM pass를 구성하고, system call whitelist를 생성하여 스레드 별로 Read/write Permission을 제한하는 기법으로 보인다. HODOR은 기존 기법보다 73.59% exploit 실행을 완화한다고 말하고 있다.

이 발표는 예전에 연구실에서 동기가 npm 연구해볼까 한다는 얘기를 들은 것 같아서, 어떤 식으로 연구를 진행하는지 궁금하여 들어보았다. System call을 제한하고, 사용되지 않는 코드를 지우는 것은 어떻게 보면 당연한 얘기 같아서 쉽게 받아들여졌지만, 발표에서 제안한 기법은 node.js의 구조를 잘 몰라 아직 이해하진 못했다. 이런 연구도 있다는 점에서 다양한 분야를 볼 수 있었다.

3. 여행

컨퍼런스 기간동안 직접 계획을 세워 다니긴 힘들고 찾아볼 시간도 없어서 일일 투어를 신청해 다녔다. 총 2가지의 투어를 하였는데, 야경투어와 랜드마크 워킹 투어를 하였다. 각 투어에서 본 것에 대해 적어보았다.

3.1 야경 투어

야경투어는 저녁 5시에 모여 영국의 주요 랜드마크를 걸어 다니면서 보는 투어이다, 세인트 폴 대성당에서 시작하여, 무슨 미술관 건물, 셰익스피어 극장, 타워브릿지, 런던아이, 크리스마스 마켓까지 이동하였다. 이동하는 과정에서 우버 보트를 사용하였는데, 가이드님 실수로 예정된 곳에서 못내려서 엘리자베스 타워까지 볼 수 있었다. 가이드님 말로는 유럽은 11월부터 크리스마스 시즌이라고 한다. 그래서 그런지 곳곳에 트리, 장식, 크리스마스 마켓 등 많이 있었다. 크리스마스 마켓은 많이 기대를 했는데, 그냥.. 크리스마스처럼 꾸며둔 플리마켓이었다. 실망이 커서 그런지 사진도 안찍었나보다.

3.2 랜드마크 워킹 투어

랜드마크 워킹 투어는 야경투어에서 본 것을 낮에 본 것과 같다. 비슷한 풍경을 보고 각 건물 별 역사에 대한 얘기를 들었다. 물론, 하나도 기억나지 않는다. 영국의 날씨는 거의 대부분 비가 와서, 낮에 찍은 것이지만 밤과 크게 다르지 않았다. 심지어 겨울이라 해도 4시면 떨어져서, 거의 빛을 못본 것 같다. 야경투어와 다른 점은 근위병 교대식을 본 것이었다. 영상으로 보는 것과 다를 게 없지 않나 했었는데, 확실히 웅장함은 달랐다. 이래서 영상과 현실은 다르다고 하는 것 같다.

투어 후 시간이 남아 쇼핑을 했는데, 포트넘앤메이슨 백화점은 티 브랜드인 포트넘앤메이슨 제품만 있었다. 2개의 층이 티와 관련된 제품만 팔고 있었다. 또, 햄리스 장난감 백화점을 갔는데 5-6층의 건물 전체에 장난감만 팔고 있었다. 볼 거리는 많았지만 살만한 것은 없었다.

3.2 음식

영국 대표 음식이라 하면 가장 먼저 나오는 것이 피시 앤 칩스이다. 그래서 피시 앤 칩스를 먹어보았다. 보통 나는 해외여행가면 입맛에 맞지 않아 잘 못 먹는 편인데, 튀긴 건 신발도 맛있다는 말이 있듯 튀긴 음식이라 그런지 괜찮게 먹었다. 이후 먹은 음식은 대부분 햄버거이고, 런던은 커리가 가장 맛있다는 친구의 말을 듣고 간 커리 음식점도 나쁘진 않았다. 하지만 가격을 생각하면, 나쁜 것 같기도 하다. 물가가 너무 비쌌다. 피시 앤 칩스 2개에 콜라 2잔하여 50파운드 정도 나온 것으로 기억한다.

4. 마무리

첫 해외 컨퍼런스로 해킹 컨퍼런스에 참석하여 구글, 텐센트 등에서 연구하는 해커들의 분석, 연구 흐름 등을 현장에서 들을 수 있는 좋은 경험이었다. 잘하고 싶다는 자극을 많이 받았다. 컨퍼런스 기간 중 FSE 결과가 나와서 더 잊을 수 없는 경험이 될 것 같다.

2024년도는 CVE를 획득해 블랙햇에 발표자로 참여해보고 싶다는 생각을 갖게 되었다. 블랙햇은 발표자와 참여자가 이름표에서부터 차이가 있었다. 발표자의 경우 이름표 맨 밑에 초록색 띠로 SPEAKER라고 적혀 있었다. 한 세션 발표장에서 본 것인데, 앉아있는 사람의 이름표로 다른 세션 발표자인 것을 보고 그 사람에게 질문을 하는 사람들이 있었다. 발표자는 질문을 듣고 막힘 없이 대답해 주는 것을 보고 열심히 해서 발표자로 오고 싶다는 생각을 하게 되었다. 기술적인 부분에선 많이 이해하진 못하였지만, 자극을 받을 수 있도록 동경해오던 컨퍼런스에 참석하는 기회를 주신 교수님께 감사드린다는 말씀을 전하고 싶다.