Black Hat Europe 2023 Trip Report

Excel London / United Kingdom

개요

2023년 12월에 컴퓨터 보안 분야에서 손꼽히는 컨퍼런스인 Black Hat Europe에 참석했다. 이 컨퍼런스는 다양한 보안 관련 주제들에 대한 심도 있는 브리핑과 함께, 여러 유명 기업들이 참여하는 비즈니스 홀 행사로 구성되어 있었다. 이는 컴퓨터 보안 업계의 최신 동향을 파악하고, 업계 전문가들과의 소통을 가능하게 하는 중요한 장이었다.

이전에도 보안 분야의 다른 중요한 컨퍼런스인 CCS에 참석한 경험이 있었기에, Black Hat Europe과의 비교가 자연스럽게 이루어졌는데, CCS에 비해 Black Hat Europe는 규모 면에서 훨씬 더 크고 다양한 프로그램이 제공됐다. 그러나 CCS 때와 마찬가지로 이번 Black Hat Europe도 많은 발표가 원격으로 진행되었는데, 이는 현장에서 직접 발표를 듣는 것보다는 현장감이 떨어졌기 때문에 아쉬움을 남았다.

그럼에도 불구하고, 이번 컨퍼런스는 다양한 분야의 전문가들과 실무자들과의 직접적인 네트워킹 기회를 제공했으며, 이는 매우 유익한 경험이었다. Black Hat Europe 2023은 단순히 연구 발표의 장을 넘어, 다양한 분야의 업계 관계자들이나 연구자들과의 네트워킹을 경험할 수 있는 특별한 경험이었다.

Conference – 흥미로웠던 발표들

Kidnapping Without Hostages: Virtual Kidnapping and the Dark Road Ahead
Craig Gibson, Vladimir Kropotov

이 연구는 '인질 없는 납치'라는 개념인 HPC(Human Process Compromise)에 초점을 맞추고 있다. HPC는 기술적 수단이나 사회 공학을 통해 대상을 오프라인 상태로 만든 후, 범죄자들이 그 사람의 친척들에게 연락하여 몸값을 요구하는 상황을 말한다. 납치범들은 ChatGPT와 같은 생성 AI를 포함한 다양한 고도의 기술적 수단을 사용하여 납치된 사람에 대한 가짜 증거를 만들어 내고, 가족들에게 몸값을 요구한다.

이 연구에서는 범죄자들이 사용하는 다양한 도구와 기술, 실제 가상 납치 사례들을 상세히 설명했다. 또한, 이러한 가상 납치 시도로부터 피해자를 보호하기 위해, 이러한 상황을 대처하기 위한 위험 신호와 조치들을 제안하고 있다.

이 연구는 매우 흥미로웠다. 다크웹에 관한 이전 연구에서는 이러한 HPC 개념을 고려하지 못했었는데, 이 연구를 통해 다크웹 연구에 HPC를 접목할 수 있지 않을까 하는 아이디어를 얻었다. Black Hat 컨퍼런스에 참여하며, 이와 같은 독창적인 아이디어를 가진 연구자들이 많다는 것을 다시 한번 깨닫게 되었다.

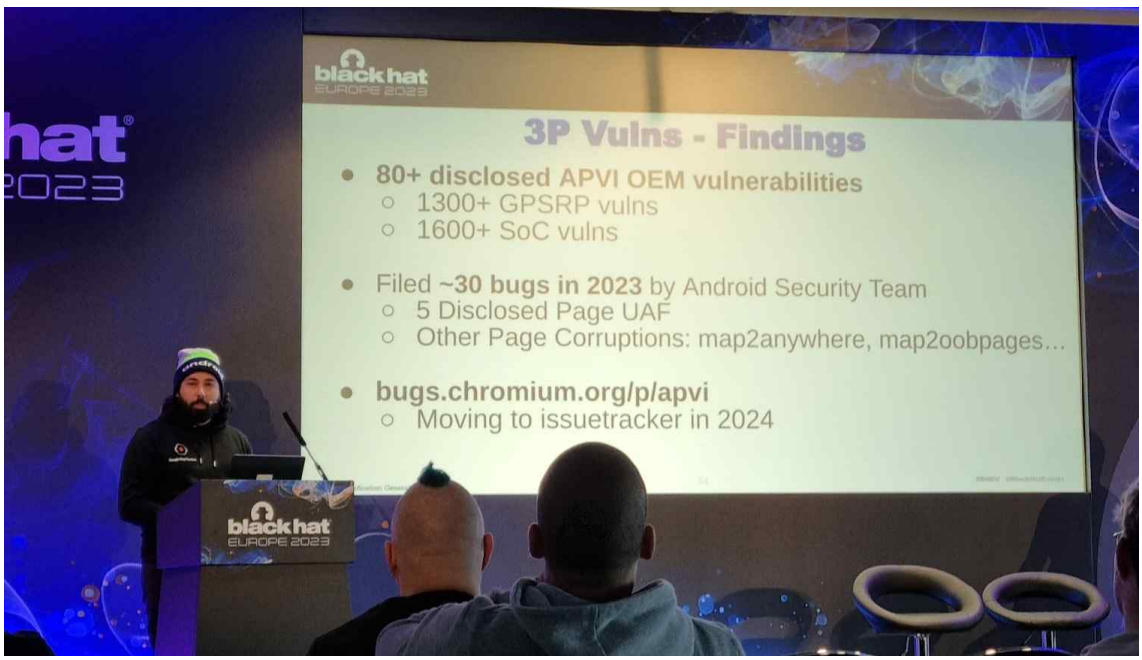
Evils in the Sparse Texture Memory: Exploit Kernel Based on Undefined Behaviors of Graphic APIs

Xingyu Jin, Richard Neal, Tony Mendez

이 연구는 안드로이드 게임의 그래픽 처리에 중요한 역할을 하는 소프트웨어 라이브러리의 취약점에 관한 연구이다. 이 라이브러리들은 그래픽을 처리하기 위해 컴퓨터의 주요 부품인 CPU와 GPU 사이에서 메모리 관리를 담당한다. 연구는 특히 그래픽 처리에 있어서 중요한 기능 중 하나인 'GPU sparse texture memory' 기능에서 발견된 여러 버그에 초점을 맞추고 있다.

'GPU sparse texture memory' 기능은 리소스가 다수의 가상 페이지를 소비하는 것처럼 보이지만 실제로는 소수의 물리적 페이지만 할당되도록 하여 물리적 메모리 페이지의 사용량을 줄이기 위해 설계되었다고 한다. 하지만 이 기능이 제대로 구현되지 않았을 때, 메모리 관련 문제가 발생할 수 있는데, 연구진은 특히 Imagination Technologies의 PowerVR GPU라는 그래픽 처리 장치에서 이런 문제를 발견했다.

해당 연구를 통해 이 장치에서 Use After Free (UAF) 취약점을 여러 개 발견했는데, 이 취약점을 통해 해커들은 메모리 관리 시스템을 조작하여 장치에 악영향을 미칠 수 있다. 이 발표에서는 이 취약점을 어떻게 악용할 수 있는지, 그리고 이를 어떻게 탐지하고 방지할 수 있는지도 설명해줬다.



Indirect Prompt Injection Into LLMs Using Images and Sounds

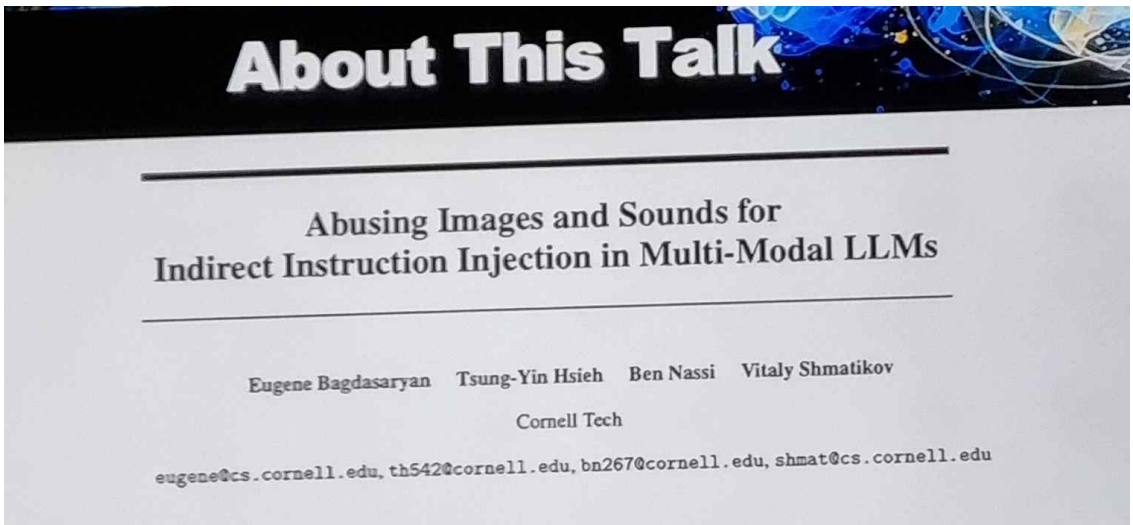
Ben Nassi, Eugene Bagdasaryan

해당 발표에서는 다중 모델 대규모 언어 모델 (Multi-modal Large Language Models, LLM)을 활용하여 보안 공격을 수행하는 방법에 관한 내용이 소개되었다.

LLM은 텍스트, 오디오, 이미지 등 다양한 입력을 결합하여 문맥이 풍부한 응답을 생성할 수 있는 고급 인공 지능 모델이다. 이러한 모델을 이용하여 공격자는 이미지나 오디오에 프롬프트와 명령을 간접적으로 주입할 수 있다. 사용자가 모델에게 변형된 이미지나 오디오에 관한 질문을 하면, 해당 미디어는 모델을 조작하여 공격자가 선택한 텍스트를 출력하도록 하거나 후속 대화가 공격자의 지시를 따르도록 유도한다.

해당 발표에서는 이러한 공격의 가능한 위협 모델과 두 가지 유형의 공격(지정된 출력 공격 및 대화 독려)을 논의하며, 이러한 방법의 기술적인 구현을 설명했다. 또한, 이러한 공격을 가장 널리 사용되는 두 개의 오픈 소스 LLM (LLaVa 및 PandaGPT)에 적용하여, 이 두 모델을 다음과 같이 조작하는 방법을 시연했다.
(1) 사용자가 위험한 웹사이트를 방문하도록 조작 (피싱), (2) 개인 식별 정보를 제공하도록 조작 (정보 수집), (3) 조작된 콘텐츠를 배포, (4) 영화 캐릭터처럼 답변 (해적, 해리 포터).

지금까지 LLM을 연구에 접목한다고 생각할 때 LLM을 보안 분야에 어떻게 적용할 수 있을지에 대해서만 생각해봤었는데 생각을 달리하여 LLM 자체에 공격을 수행한다는 것이 흥미로웠다. 해당 연구에 관한 논문이 아카이브에 게재되어 있어 읽어볼 예정이다.

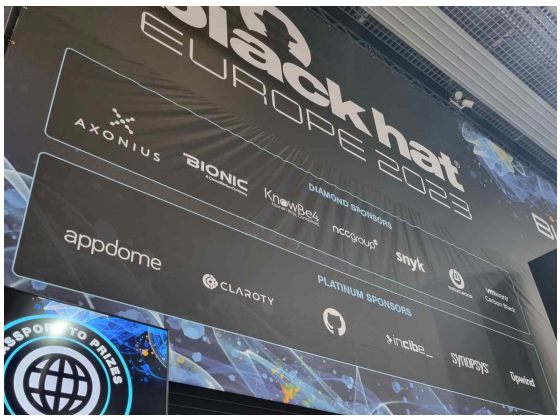


Conference – Business Hall

Black Hat은 다른 학회들과는 달리 특별한 행사를 진행하는데, 그중 하나가 바로 Business Hall에서 열리는 행사이다. 이 홀은 보안 전문가, 연구원, 솔루션 제공업체들이 마련한 부스들로 가득 차 있어, 각 기업이 어떤 일을 하는지, 해당 분야의 최신 경향은 무엇인지에 대해 직접 이야기를 듣고 교류할 기회를 가질 수 있었다. 다들 너무 친절하게 설명해주신 덕분에 다양한 전문가들과의 네트워킹을 할 수 있는 좋은 기회였다.

또한, Business Hall 내에 있는 Black Hat Store는 다양한 종류의 기념품들로 가득 차 있어 많은 참가자의 관심을 끌었다. 이곳에서는 Black Hat 테마의 티셔츠, 모자, 기념품 등 다양한 상품들을 구매할 수 있었는데, 사람들이 이 기념품들을 실제로 구매했다. 컨퍼런스의 마지막 날에는 일부 인기 상품들이 매진되어, Black Hat의 높은 인기를 다시 한번 확인할 수 있었다.

이렇듯 Black Hat은 보안 분야의 최신 정보를 공유하고, 다양한 기술과 솔루션을 직접 체험할 수 있는 장소였다. Business Hall의 부스 방문을 통해 실제 업계의 다양한 측면을 탐색할 기회가 제공되었으며, Black Hat Store의 다양한 기념품들을 통해 이 컨퍼런스만의 독특한 경험을 기념할 수 있었다.



여행기

런던의 거리

컨퍼런스의 메인 브리핑이 없는 날은 런던을 여행했다. 런던에도 소매치기가 많다고 해서 만반의 준비를 하고 런던의 거리로 나왔다. 물론 소매치기가 없지는 않았지만, 위험한 정도는 아니었고 거리를 메우는 크리스마스 장식들과 캐럴로 가득해서 거리를 걷는 것만으로 기분이 좋아졌다. 그런데 정말 그 명성답게 런던에 있는 동안 맑은 하늘은 본 날이 하루밖에 없었는데 정말 영국답다는 생각이 들었다.

런던의 음식

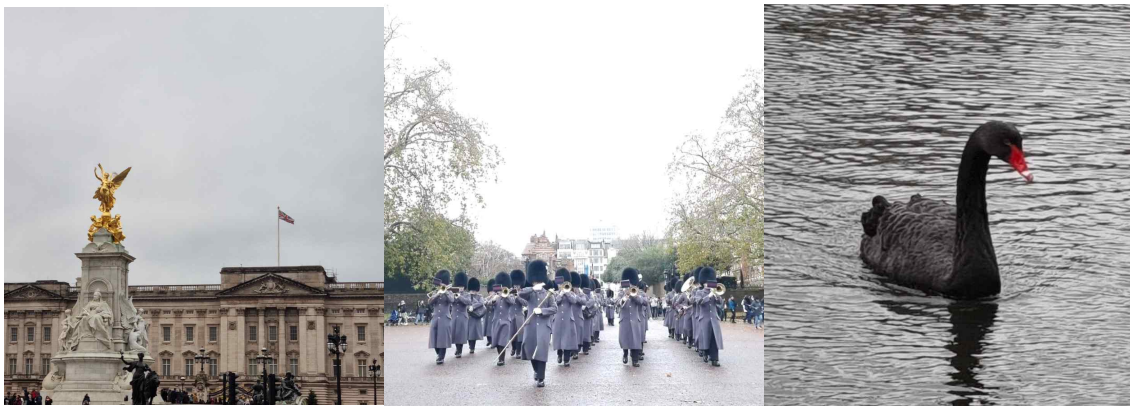
영국의 음식에 대한 악명과는 달리, 음식이 맛있었다고 기억한다. 물론, 높은 물가 때문에 대부분의 식사를 간단히 해결했지만, 영국의 대표 음식인 피쉬앤칩스와 커리 그리고 스콘 등을 먹어봤다. 두 요리는 매우 맛있었고 스콘도 정말 맛있어서, 런던에서의 기억을 더욱 특별하게 만들어줬다.

런던의 야경

런던의 야경을 감상하기 위해 주요 관광지를 돌아보기로 했다. 타워 브릿지, 빅벤, 런던 아이 등 런던의 주요 야경 명소들을 방문했다. 영국답게 비가 내리는 날씨에도 불구하고, 화려한 야경과 거리 곳곳에 있는 크리스마스 마켓은 정말 인상적이었다. 런던의 밤은 낮에 보는 런던보다 더 아름다웠고, 이 도시의 매력을 더욱 빛나게 했다.

버킹엄 궁전

근위병 교대식을 보기 위해 버킹엄 궁전을 방문했다. 많은 사람이 이미 모여있었고, 비가 내리고 있어 교대식이 취소될까 우려되었다. 하지만 다행히 비가 그쳐서 교대식을 볼 수 있었다. 근위병 교대식은 한국의 덕수궁 수문장 교대식을 생각나게 했지만, 두 교대식은 매우 달랐고, 그 차이가 매우 흥미로웠다. 특히 인상적이었던 것은 교대를 위해 이동하는 근위병들이 매우 빠른 속도로 구보하는 장면이었다. 이를 구경하던 주변 사람들이 모두 그들을 따라 뛰어가야 할 정도로 빨랐다. 또한, 버킹엄 궁전 근처의 호수에서는 블랙스완도 볼 수 있었다.



마치며

다양한 국내외 학회 및 과제 발표회에 참석한 경험이 있지만, Black Hat에 참석하게 된 것은 그중에서도 특별한 경험이었다. 컴퓨터 보안 분야에서의 명성과 개인적인 관심이 맞물려, 이번 컨퍼런스에 대한 기대감이 컸었다. 그리고 실제로 참석해보니, 그 기대가 헛되지 않음을 깨달았다.

Black Hat에서의 발표들은 완벽하게 보안에 초점이 맞춰져 있는 발표들이 대다수였는데, 다른 연구자들이 어떤 관점에서 연구를 진행하는지 얼마나 다양하고 좋은 아이디어를 가지고 연구를 완성하는지 볼 수 있었다. 이를 통해 현재 진행 중인 연구에 대해 다시금 생각해보고, 진행 중인 연구들이 얼마나 부족했는지 인식하는 계기가 되었다. 하지만, 발표 자료가 사전에 공개되지 않아 배경지식이 부족한 주제에 대한 이해가 어려웠고, 발표 후 질의응답 시간이 없는 발표가 대다수였기에 이는 아쉬움으로 남았다. 직접 질문하지 않더라도 다양한 참가자들의 다양한 시각에서 나오는 질문들을 통해 해당 발표에 대한 이해도를 높이고 새로운 관점에 대한 의견을 듣는 것이 중요하다고 생각했는데 질문이 불가능했기 때문에, 이 부분에서는 다소 한계를 느꼈다. 이 외에도 비즈니스 홀에서의 네트워킹 기회는 매우 즐거웠지만, 영어 실력의 한계로 인해 더 깊이 있는 교류를 하지 못한 것도 아쉬웠다. 이를 통해 영어의 중요성을 다시 한번 실감하게 되었다.

그런데도, Black Hat 컨퍼런스는 새로운 경험을 제공했고, 특히 연구에 대한 동기부여를 크게 강화해주었다. 오랫동안 가지고 있던 Black Hat에 대한 로망이 실제 참가를 통해 현실이 되었고, 이는 내 연구에 대한 큰 동기부여가 되었다. 연구실에 있으며 다양한 경험을 할 수 있었는데 이런 특별한 경험을 할 수 있는 기회를 주신 교수님께 항상 감사하다고 말씀드리고 싶다.