**( 1 )주 단기현장실습 보고서**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **학부** | **컴퓨터공학부** | **전공** |  | **학번** | **2016136048** | **성명** | **박효경** |
| **실습기간** | **2018 12월 26일 ~ 2019년 01월 23일** | | | | | | |
| **실습기관** | **㈜ 달소프트** | | **부서** | **개발팀** | | | |

**2019년 1월 2일**

**본 문**

1. 현장 실습 주제

한 달 간, ㈜달소프트의 개발팀에 소속되었습니다. 팀원들과 함께 대표적인 동영상 스트리밍 사이트 YouTube, Vimeo, Twitch의 영상을 통합 검색하여 사용자에게 이에 대한 결과를 조회할 수 있도록 하는 웹 사이트 구축 프로젝트를 진행하라는 업무 지시를 받았습니다. C# 언어, Java Script, CSS, HTML 언어를 기반으로 하여 ASP.NET Core 2.0, Vue.js, Ms SQL 등을 사용하고자 합니다.

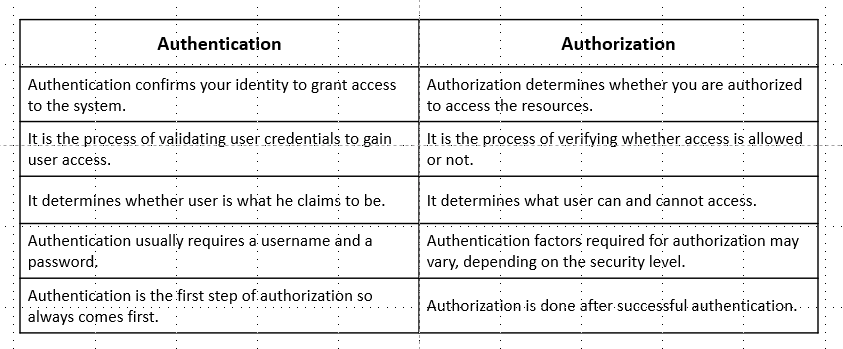
1. 학습 내용

Authentication과 Authorization의 차이, Oauth 2.0과 JWT, REST API, 공개 키 암호화 알고리즘, 대칭 키 암호화 알고리즘 등 각종 기술 조사를 실시했습니다. 동영상의 목록을 받아 오기 위하여 YouTube Data API v3, Vimeo API, Twitch API 사용법에 대하여 숙지했습니다.

1. Authentication과 Authorization의 차이

**Authentication**은 사용자가 누구인지 증명을 하는 프로세스로, 로그인 form, HTTP authentication, HTTP digest, X.509 등에 사용됩니다. (Authentication is any process by which you verify that someone is who they claim they are)

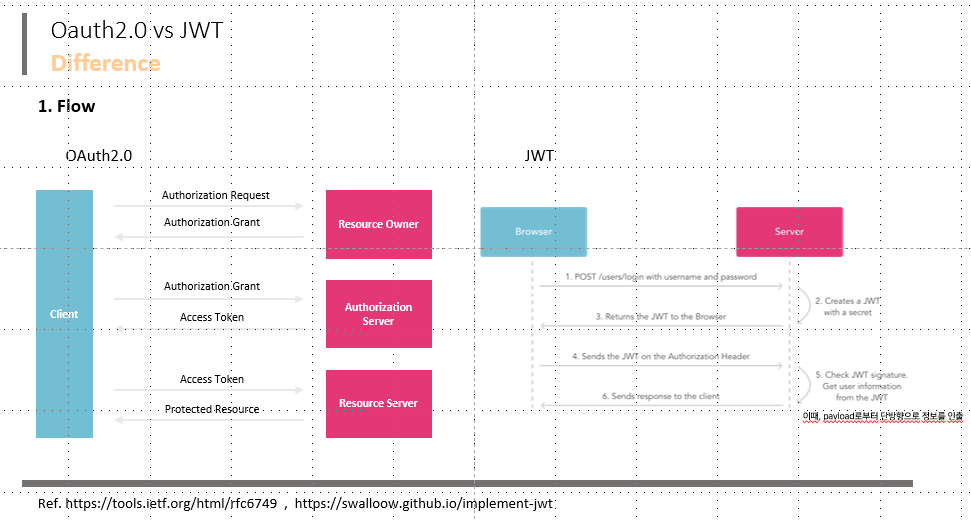
**Authorization**은 사용자가 어떠한 행위를 할 수 있도록 권한을 허가(부여)하는 프로세스, URL들을 제거할 수 있는 접근 권한을 부여, 오브젝트와 메소드들의 보안과 관련된 권한을 부여하는 것을 의미합니다.(Authorization is any process by which someone is allowed to be where they want to go, or to have information that they want to have)



1. Oauth 2.0과 JWT

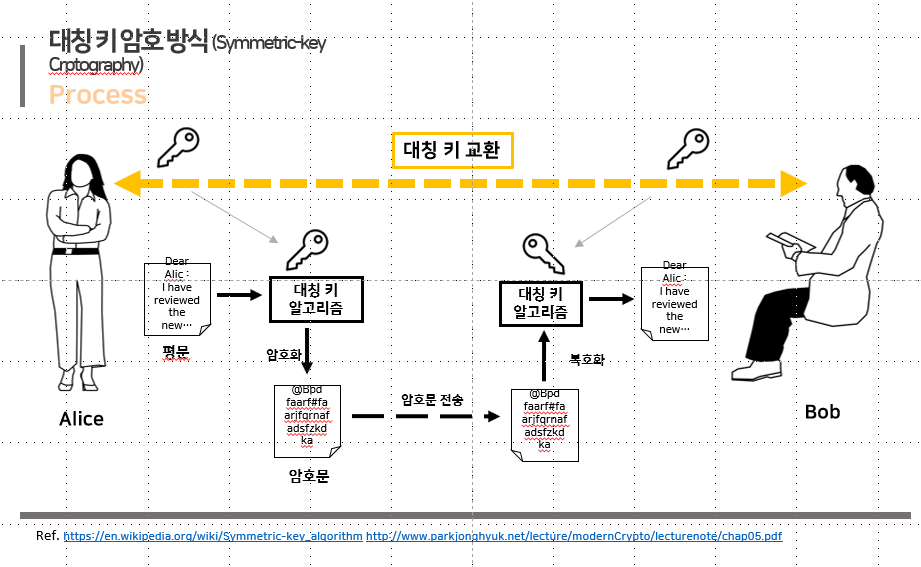
**Oauth 2.0** the industry-standard protocol for authorization.

**JSON Web Token (JWT)** is an open standard ([RFC 7519](https://tools.ietf.org/html/rfc7519)) that defines a compact and self-contained way for securely transmitting information between parties as a JSON object.

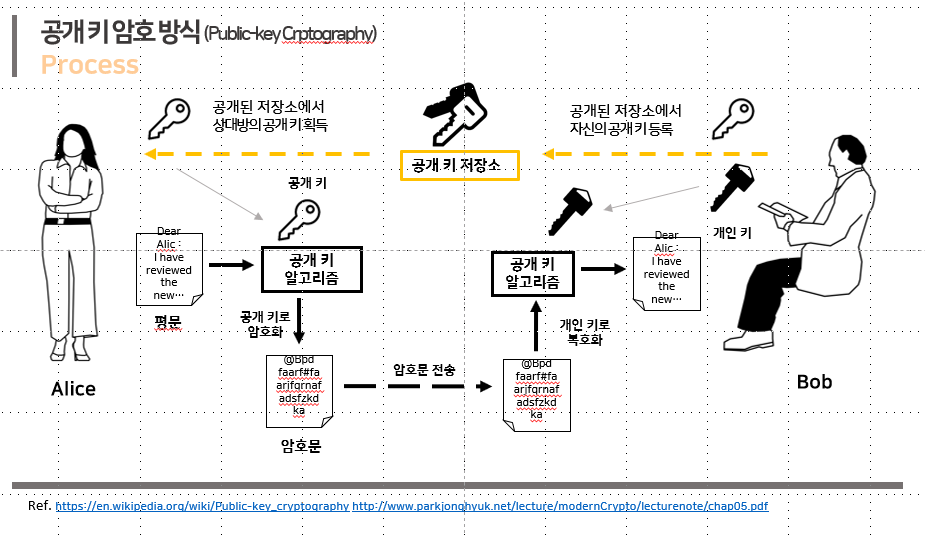


1. REST API
2. **대칭 키 암호화 알고리즘**

암호화 방식의 한 종류로, 암호화와 복호화에 같은 암호키를 사용하는 알고리즘을 의미합니다. 아래의 예시에서 Alice가 Bob에게 암호화 된 메시지를 보낸다고 가정을 할 때, 사전에 Alice와 Bob은 대칭 키를 교환한 후, Alice가 평문을 사전에 공유한 대칭 키를 이용한 알고리즘을 통해 암호화를 진행하고, 이 암호문을 Bob에게 전송합니다. 정송 받은 암호문을 Bob은 다시 가지고 있던 대칭 키를 활용하여 복호화를 하고 평문을 해석하게 되는 과정을 거칩니다.



1. **공개 키 암호화 알고리즘**

암호 방식의 한 종류로, 암호화와 복호화에 서로 다른 키를 사용하는 암호화 방식입니다. 대칭 키 암호화 방식과 비교하여 ‘비대칭 키 암호화 알고리즘’이라고도 불립니다. 다시, Alice가 Bob에게 암호화 된 메시지를 보낸다고 가정할 때, 우선 Bob은 공개된 공개 키 저장소에 본인의 공개 키를 등록시킵니다. Alice는 공개된 저장소에서 상대방의 공개 키를 획득하고 이 공개 키를 통한 알고리즘을 이용해 평문을 암호문으로 변환하는 작업을 가집니다. Bob에게 만들어진 암호문은 전송하면 Bob이 원래 가지고 있던 개인 키로 복호화하여 평문을 읽을 수 있도록 하는 과정을 거칩니다. 대표적인 공개 키 암호 방식의 예로는 **RSA**가 있습니다. 1978년 Ron Rivest, Adi Shamir, Leonard Adleman의 연구에 의해 체계화된 자연 소인수 분해를 기반으로 한 공개 키 암호 방식입니다. **ElGamal**이란, 타헤르 엘가말이 1985년에 고안한 Diffie-Hellman key exchange 이론을 바탕으로 한 공개 키 암호 방식입니다. 이를 이용하면 메시지의 길이가 2배로 늘어난다는 단점이 있습니다. **ECC**란 Eliptic Curve Crypto System의 약자로, 타원 곡선 암호 시스템이라 불립니다. 타원 곡선 이론에 기반하여 1985년 닐 코블리츠와 빅터 밀러가 각각 독립적으로 제안한 공개 키 암호 방식입니다. 이때 타원 곡선이란 아래의 방정식을 만족하는 모든 점들의 집합을 의미합니다.

**전자 서명**이란 서명자를 확인하고 서명자가 당해 전자문서에 서명했다는 사실을 나타내는 데 이용하려고, 특정 전자문서에 첨부되거나 논리적으로 결합된 전자적 형태의 정보를 의미합니다. 디지털 서명과 전자 서명을 다른 의미를 지니는데, 디지털 서명이란 전자 서명을 통해 서명자를 확인하고 인증하는 모든 행위를 의미하며, 전자 서명의 경우는 디지털 서명을 하기 위한 정보를 의미합니다.

1. **Youtube Data APi v3, Vimeo API, Twitch API 활용**

EX1) Vimeo, Twitch, Youtube Search API TEST

<https://www.getpostman.com/collections/72092716ce4fac5689f8>

EX2) Youtube Activities API TEST (사용자 맞춤 설정 HOME 피드, 이벤트 등 조회)

<https://developers.google.com/apis-explorer/?hl=ko#search/youtube%20activities/m/youtube/v3/youtube.activities.list?part=snippet&home=true&maxResults=50&_h=2&>

1. 소감

모든 경험이 처음으로 겪는 것들이기에 매우 새로웠고, 소중했습니다. 출근을 하기 위해 아침 첫 차를 타고 천안역에서 1호선 지하철을 타고 가산 디지털 단지역까지 올라오면서 만나는 모든 사람들도 새롭게 보였습니다. 회사라는 곳은 무슨 일이라도 팀 단위로 이루어지기 때문에, 사소한 것 하나까지도 팀원들과 회의를 거쳐 진행해야 했습니다. 멘토이자 대표님께서 직장 생활에 대한 예절, IT 업계에서 성장해 나가기 위한 팁이나 프로젝트 진행 시 필요한 기본적인 소양에 대해 말씀해 주셨고, 많은 도움이 되어 감사했습니다. 개발자 분들 앞에서 세미나를 진행하는 것은 매우 어렵고 힘든 일이라는 것을 깨닫게 되었고, 학부생 수준을 뛰어 넘어 준비해야 했습니다. 세미나를 진행하기 위해 밤을 새며 준비하고, 자료조사를 진행하면서 이해하기에 너무 어려운 내용들이 나왔으나 몇 번이고 다시 보며, 이에 개인적으로 전공 지식을 더욱 탄탄히 쌓을 수 있었던 것 같습니다.

1. 세미나 발표 자료

18.12.31

<https://drive.google.com/open?id=1g4X4AzkBTjfGL4N64CWFxyog1PbGc4Fw>

19.01.02

<https://drive.google.com/open?id=1gSP6TmPxWECFgqAnaRB13sshoNkYE-TC>