

2018/10/16, 3-2 Capstone Project

RabbitMQ 취약점 분석

- 보안 취약점 분석 및 보완 프로그램 개발 -



지도교수 : 이종혁

Captain : 201621571 손상진

Sailors : 201621110 권순홍

201621136 서민지

201621173 최서윤



QBQB

목차

1. 주제 소개

- 선택 배경
 - 오픈소스 메시지 브로커
 - RabbitMQ를 사용하는 서비스
 - 취약점
 - 알려진 취약점
- 목표
 - 취약점 분석 기법



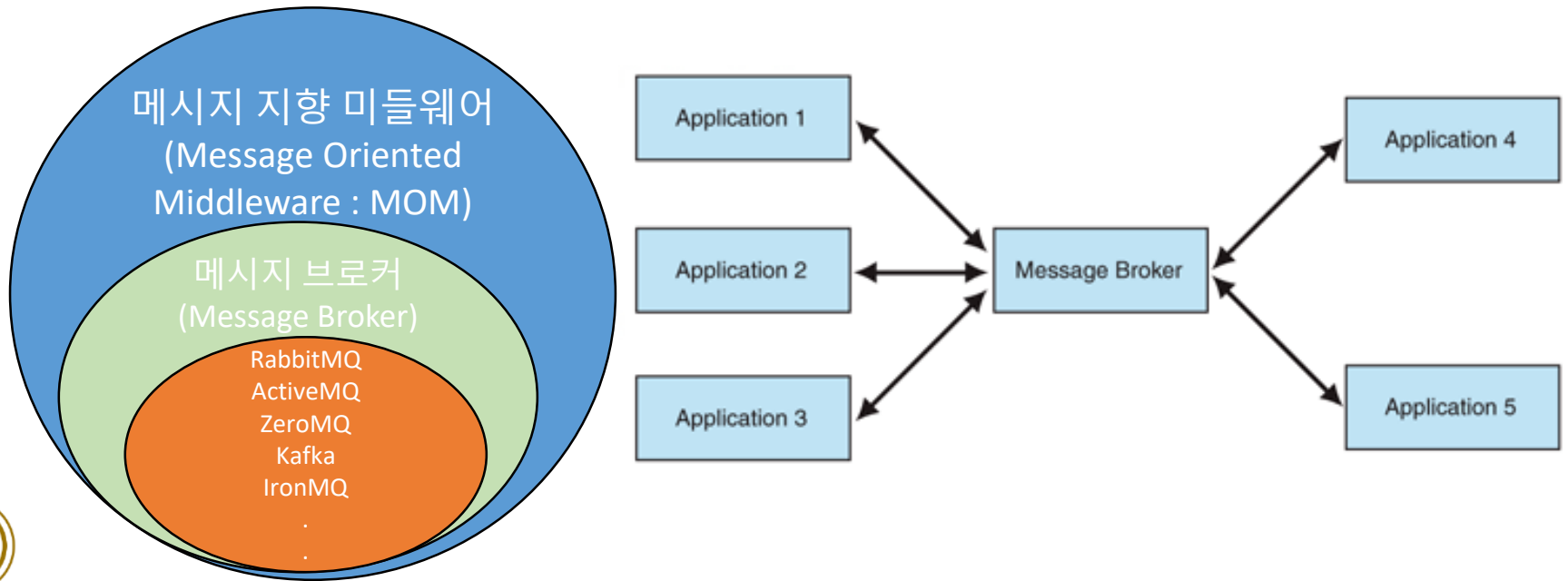
2. 진행

- 진행 사항
- 앞으로의 진행 계획

1. 주제 소개

- 선택 배경

- 최근 증가하는 트래픽에 따른 메시지 사용량 증가로 메시지 브로커를 사용
 - 비동기 메시지를 사용하는 프로그램 사이에서 데이터의 송수신

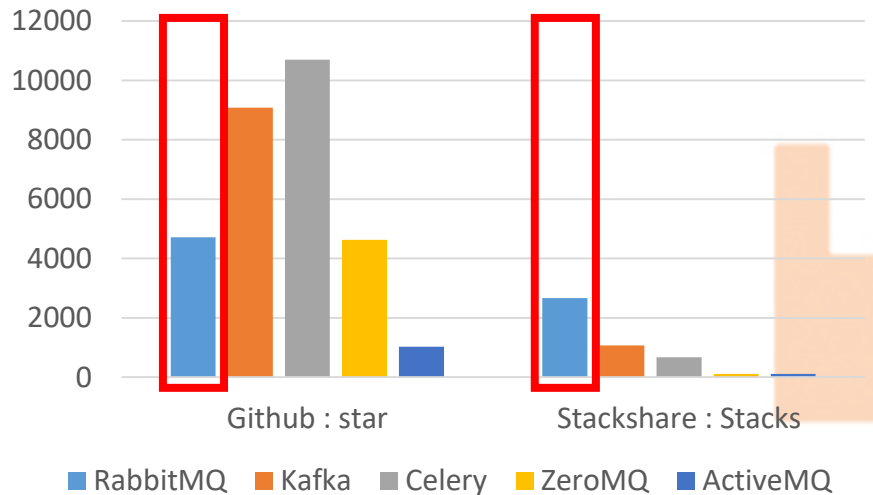





1. 주제 소개

- 선택 배경

- 다양한 오픈소스 메시지 브로커 존재

오픈소스 메시지 브로커의 인기



	 RabbitMQ <small>by Pivotal</small>		
	RabbitMQ	Kafka	ActiveMQ
언어	Erlang	Java, Scala	Java
년도	2007	2011	2004
라이선스	MPL	Apache2.0	Apache2.0
특징	빠름, 뛰어난 측정 및 모니터링, 많은 사용자	높은 처리량	사용이 쉽고, 빠름
사용	750개의 회사	341개의 회사	29개의 회사

1. 주제 소개

- 선택 배경

- RabbitMQ를 사용하는 서비스

- Reddit



다양한 주제에 걸친 뉴스 및 토론 콘텐츠가 업로드 되며
세계 32위의 커뮤니티 플랫폼으로 한 달 평균 1억 6천명이 방문



- Trivago



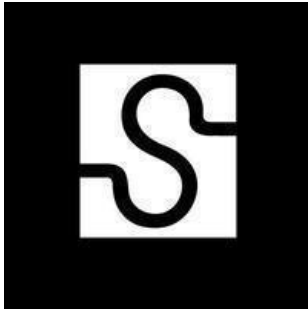
호텔 및 호스텔 등 다양한 숙박시설 요금을 비교하는 독일의 메타 검색
엔진으로 월 평균 1억 2천만명의 방문자가 웹사이트를 이용

1. 주제 소개

- 선택 배경

- RabbitMQ를 사용하는 서비스

- Sauce Labs



클라우드 호스팅 및 웹, 모바일 애플리케이션 자동화 플랫폼

- Yammer



기업용 소셜 네트워크 서비스로 메시지를 공개적으로 내보내는 SNS와 달리 폐쇄적 그룹내의 구성원들끼리 사용할 수 있음

1. 주제 소개

- 선택 배경

- RabbitMQ를 사용하는 서비스

- Zillow



온라인 부동산 웹사이트로 같은 업계 사이트들 중 최다 방문자 수를 자랑하며 주택 매물 정보를 실시간으로 전달



- 이외에도

COMPANIES USING RABBITMQ



+ 931 more

Login to see more stacks

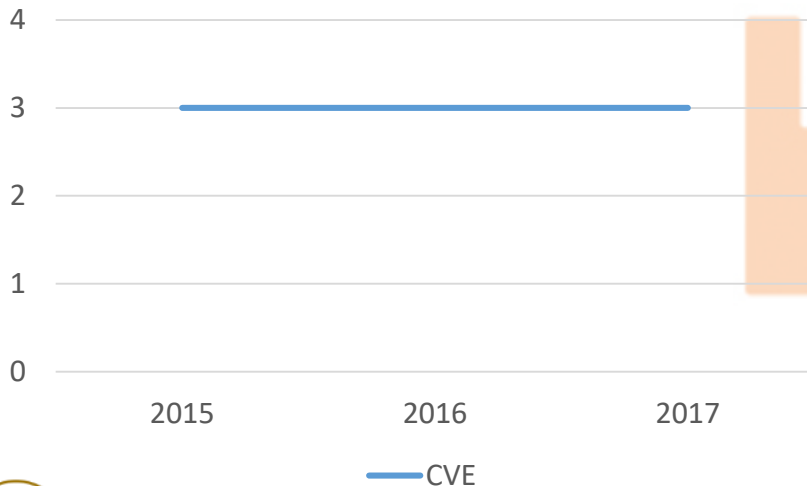
1. 주제 소개

- 선택 배경

- 그런데...

- 매년 꾸준히 RabbitMQ의 보안 취약점이 발견되고 있음.

년도 별 취약점 수

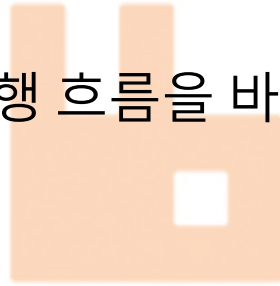


Vulnerability Trends Over Time

Year	# of Vulnerabilities	DoS	Code Execution	Overflow	Memory Corruption	Sql Injection	XSS	Directory Traversal	Http Response Splitting	Bypass something	Gain Information
2015	3						1		1	1	
2016	3	1									1
2017	3						2				
Total	9	1					3		1	1	1
% Of All		11.1	0.0	0.0	0.0	0.0	33.3	0.0	11.1	11.1	11.1

1. 주제 소개

- 보안 취약점이란?
 - 보안 취약점(Security Vulnerability)
 - s/w나 정보시스템 상에 존재하는 보안상의 결점
 - 프로그램을 본래의 기능과 다르게 동작하게 하거나, 허용된 권한을 초과, 의도하지 않은 오류를 일어나게 할 수 있는 조건들
 - 익스플로잇(Exploit)
 - 취약점을 이용하여 실행 흐름을 바꿀 수 있도록 하는 과정 or 코드



1. 주제 소개

- RabbitMQ의 알려진 보안 취약점(1/2)

- DoS(Denial of service)

- CVE-2015-8786
 - 년도: 2015
 - 스코어 : 6.8
 - 3.6.1 이전 버전에서 관리 플러그인을 사용하면 특정 권한을 가진 원격인증 사용자가 몇몇 개개 변수를 통해 서비스 거부를 발생시킬 수 있음

- Gain Information

- CVE-2016-0929
 - 년도 : 2016
 - 스코어 : 5.0
 - 실패한 명령들이 로그에 기록 되므로, 중요한 정보를 얻을 수 있음



1. 주제 소개

- RabbitMQ의 알려진 보안 취약점(2/2)

- Cross Site Scripting (XSS)

- CVE-2017-4967
 - 년도 : 2017
 - 스코어 : 4.3
 - 3.6.9 이하 버전의 관리 UI에서 사이트에 악의적인 스크립트를 넣어 공격하는 XSS 공격 취약점

- Authentication

- CVE-2016-9877
 - 년도 : 2016
 - 스코어 : 7.5
 - 3.6.6 이하 버전에서 MQTT(IoT에서 사용되는 메시지 프로토콜) username/password 쌍으로 연결 인증을 성공한 경우 password가 누락되어도 인증 성공하는 취약점



1. 주제 소개

- 목표

1. RabbitMQ 프로그램 분석 및 문서화
 - github의 오픈소스 및 CloudAMQP의 문서 분석
 - github를 사용하여 문서화
2. RabbitMQ 취약점 분석 및 취약점을 보완
 - 취약점 분석 기법 사용
3. 취약점을 보완한 프로그램 적용 및 테스트
 - 오픈소스인 RabbitMQ + 취약점 보완 = 프로그램

1. 주제 소개

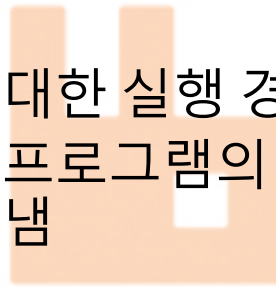
- 취약점 분석 기법(1/2)

- Fuzzing(Fuzz testing)

- 소프트웨어에 무작위로 값을 반복적으로 하여 에러가 발생하면 원인을 분석해 보안 상의 취약점을 찾는 방법
 - 대부분의 취약점이 Fuzzing을 통해 발견

- Symbolic Execution

- 프로그램의 입력 값에 대한 실행 경로를 분석하기 위한 기법
 - 분기문의 조건을 보고 프로그램의 어떤 지점에서 각 변수가 어떤 값을 갖는지 알아냄



Normal execution

input: x = 4, y = 3
output: 3, 4

Symbolic execution

input: x = A, y = B

output: A, B
Path-condition: $A \leq B$

output: B, A
Path-condition: $A > B \wedge B \leq A$

1. 주제 소개

- 취약점 분석 기법(2/2)

- Taint Analysis

- 사용자 입력 값을 통해 어떤 레지스터와 메모리 영역이 제어 가능한지 확인하는 기법
 - 메모리 위치 및 레지스터의 오염(taint) 여부 확인

- 이외에도..

- Reverse Engineering
 - 소스코드 분석



2. 진행

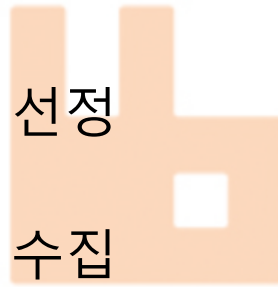
- 현재까지 진행 사항

- 9월

- RabbitMQ 개념적 이해
 - RabbitMQ 설치 및 테스트
 - RabbitMQ 사용


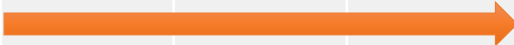
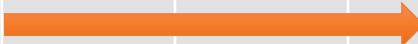
- 10월

- RabbitMQ를 통한 주제 선정
 - 초안 발표
 - RabbitMQ 취약점 정보 수집



2. 진행

- 앞으로의 진행 계획

	10월	11월	12월	1월	2월	3월	4월	5월
RabbitMQ 분석								
RabbitMQ 보안 취약점 분석								
취약점을 보완한 프로그램 개발								



2. 진행

- 앞으로의 진행 계획

- 18년 2학기

- RabbitMQ가 제공하는 기능에 대해 분석 및 실습
 - 플러그인 확장하여 사용
 - 소스코드 구조 분석 및 문서화
 - 예제 코드를 활용하여 레이턴시 비교
 - 다른 MQ와 비교
 - 관련 기술 동향 수집



2. 진행

- 앞으로의 진행 계획

- 19년 1학기

- 보안 기능 추가

- RabbitMQ 보안 관련 기능 분석 및 정리
 - SSL/TLS을 통한 메시지 프로토콜 적용
 - 추가적으로 필요한 기능 덧붙이기

- 애플리케이션 개발

- 추가 기능 RabbitMQ 소스를 기반으로 추가 후 최적화

