

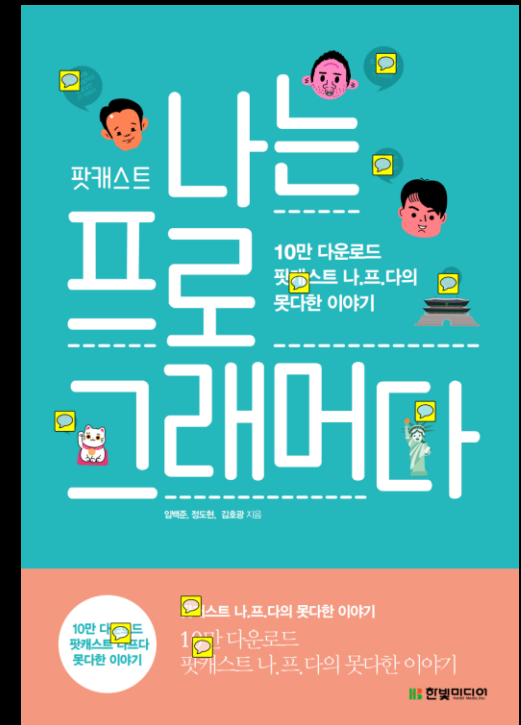
스타트업에서 사용하는 오픈 소스와 보안

Dennis Kim



Who am I ?

- 2015. Makeus Mobile CTO
- 2015. 팟캐스트 나는 프로그래머다 MC
(팟캐스트2등)
- 2014. Microsoft MVP, Azure
- 2014. Nike Run the city PM
- 2012. 라이브플렉스 CTO
- 2010. 드래곤볼 온라인 보안



보안과 해킹하며
서비스를 만드는 사람

약 10년 전

은행
인터넷 간편 계좌
조회는
없어졌습니다

이름 계좌 번호

4자리 비밀번호

중

2자리

잔액 조회 가능

K은행 앞 2자리

W은 행 뒤 2자리

재미있는 건...

패스워드 실패
5회 **Block**

PW 실패 4회
IE 닫기.

실패 회수 초기화

27개의 은행

각각 100회

계좌 **PW** 획득!!

간단한 휴먼
에러

보안을 모르는
안일한 개발

간편 계좌 조회
폐지!

소비자는 불편!

보안은 강화!

이것_이 해커_의 일!

Hacker's way!

Today Issue

Open Source
다양성

Open Source

취약 이야기

아님

Open Source

보안도

우수해짐!

Close == Open

비슷한 Patch
주기

**대기업 SW
개발자
Full time job**

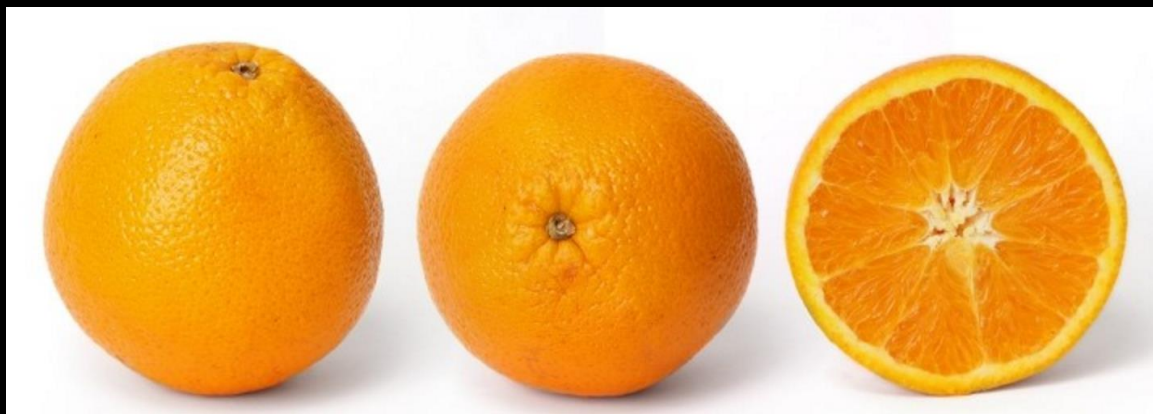
오픈 소스
기여중!

휴먼 에러

모노폴리

오늘의 키워드

오렌지



지금 부터 4개 품종

바나나

그로미셸

보다 맛없는

캐번 디시

대량 상업 생산

단일 품종 경작

취약해진 종의 생태계

단일 품종 노리
질병

파나나 병 재발

**바나나나 멸종
카운트다운!**

다양성_에 대한 화두

정말

Open Source는

다양한가?

안드로이드 게임

70% 이상

(2015년 구글 플레이 KR + kakao talk, global market 45%)

Unity 3D

2011년

15% **내외**
Unity3D

Game에만 한정?

과도한 일반화?

이런 의문에서

뜯어봤습니다

리버스 엔지니어링

구글 플레이

+

이통사 기본 앱

5분 후 결과를
공개합니다!

1990년대 월스트리트

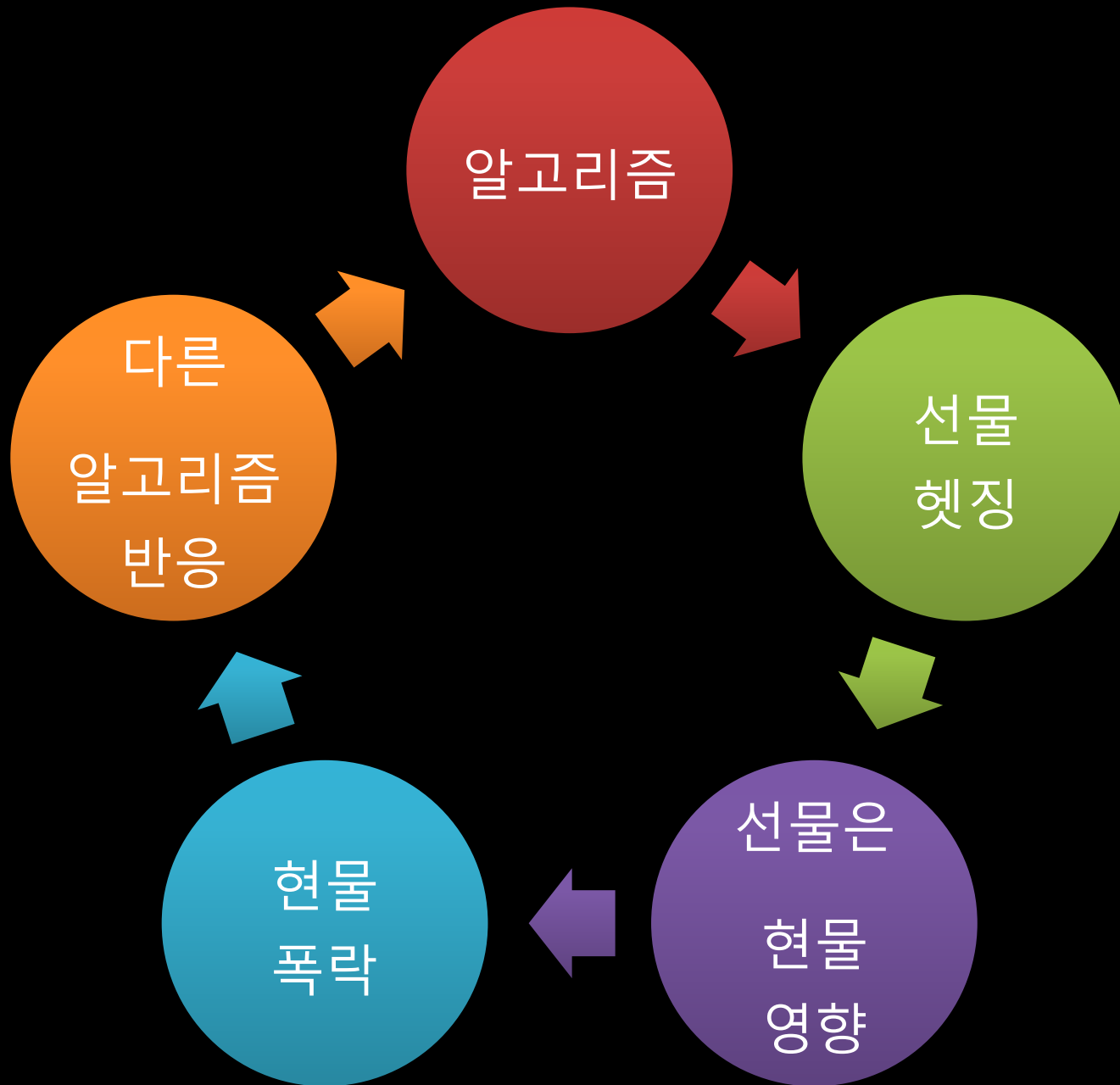
새로운
금융공학
포트폴리오
투자

선진 금융 기법

컴퓨터 알고리즘

그런데
이유없이
주식 폭락!

단 하나 개별
알고리즘 오류



독립된 로직이
트리거로 작용

goto ERROR;

무한 루프

개별 / 비슷한

SW

단일 POOL 영향

다시 앱
이야기로!

앱 클라이언트 구성 라이브러리

50~65%

동일

라이브러리

오픈 소스 기술 안정화로 해석

2010년 ~ 2012년
삼질에 시기

재미있는 시도

다양성 X

특이점

42% 구버전

25%

평문 통신

그럼
서버 사이드
기술?

궁금했습니다!

한국^의 공익^의

목적^{이라도} 보안스캔

불법

구하라
찾을 것이다!

클라우드

이용한

연변개 스미싱

포렌식

범죄의 기록 에버노트

방계 조직 사이트 발견

中国红客

进入联盟社区

红客联盟 红客联盟 红客联盟 红客联盟 红客联盟 红客联盟 红客联盟

红客联盟地址: www.chinahackers.com

红客联盟(红客中文社区): www.chinahackers.com 红客联盟(红客中文社区): www.chinahackers.com

195개 앱 분석

SSH Open **34개**

하트 블리드 영향 **57개**

워드 프레스 취약점 영향 **11개**

관리자 any 오픈 **75개**

JIRA Any 오픈 **29개**

위키 오픈 **11개**

방화벽 없는 **115개 앱**

취약점 버전 사용 **145개 앱 서버**

차세대 먹거리
분석 완료!

스미싱
대포통장 차단
지연 인출

게임머니 털기
집중!

막히면

대중 기본 앱
공격 예상

Monetize

난이도 문제!

농담일까요?

러시아->중국

랜섬웨어 사태

사이버 범죄의

글로벌 공조

가속

왜 기본 설치앱
문제일까?

삭제 불능

앱 개발
아웃소싱

과도하게 짧은
개발 기간

개발자는 없는
앱 양산

기본 설치앱_의 생태계

바나나나 와 다를 것없^는

단일 생태계

마공! 단수치기

Solution

Cloud_{플랫폼}

이용하세요!

IBM SoftLayer
security Sean

AWS WAF

그나마
클라우드_는

하트 블리드 때처럼

Patch

공개 보안 취약점 Scanner

서버 사이드 팁

점점 이 줄이세요!

ACL 관리

AWS

Azure

KT Cloud

ACL Firewall 지원

유료 Firewall
클라우드 고민하세요

마지막으로

정기적인

Open Source

Version up

유명하지
않더라도

공격 당합니다

해커_는

랜덤입니다

감사합니다!