오픈소스와 보안

2015.12.03
서울여자대학교 정보보호학과
조시행(sihaeng.cho@gmail.com)

2015년 인터넷 10대 산업 이슈 전망

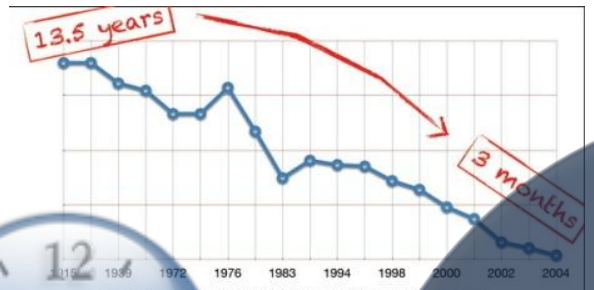
- 오감 인지하는 “Wearable Device”
- 새롭게 쓰는 인터넷 금융의 역사 “Fin-Tech”
- 초연결사회의 하이웨이 “Giga Internet”
- 디지털 금맥 찾기 “Data Scientist”
- 세계를 겨냥한 벤처 “Global Startup“ 약진
- 생산의 고정관념을 바꾸는 “3D Printing”
- **미래인터넷의 지름길 “Open Source 생태계“**
  - **오픈소스 보안 분석 프레임워크 구축 등 오픈소스 보안 강화의 중요성 증대**
  - **안전하고 신뢰할 수 있는 보안은 오픈소스 활성화에 있어 중요 요소로 예상**
- 차세대 “Neo모바일 플랫폼” 경쟁
- “중국 인터넷 기업”과의 전략적 공존
- 인터넷 인본주의의 시작 “인터넷 접근권”

출처 : 2015년 인터넷 및 정보보호 10대 산업이슈 전망(2014, KISA)

2015년 보안 전문 업체들이 예상한 주요 정보보안 이슈

- **IoT(Internet of Things) 환경에서의 보안**
  - IoT 기기 공격 증가
  - 가전제품, 스마트 카, 스마트 홈, 헬스케어 등…
- **모바일 영역 보안 위협 증가**
- **금융 관련 공격 증가**
- **SW취약점에 대한 공격**
  - **오픈 소스**
- **금전을 노린 랜섬웨어 공격**
- **개인 정보보호 관련 규정 강화**

오픈 소스



Time to Market

비용 절감

효율적 개발 및 지원

OSS의 품질

컴퓨팅 환경의 변화

1984	1989	1994	1999	2004	2009	2014	2019
Personal Computer	PC 통신	Desktop PC	Portable PC	Notebook Netbook	iPhone Android	Internet of Things	Smart CAR


Personal Computing


Text Computing


Web Computing


Internet Computing


Portable Computing


Mobile Computing


Things Computing

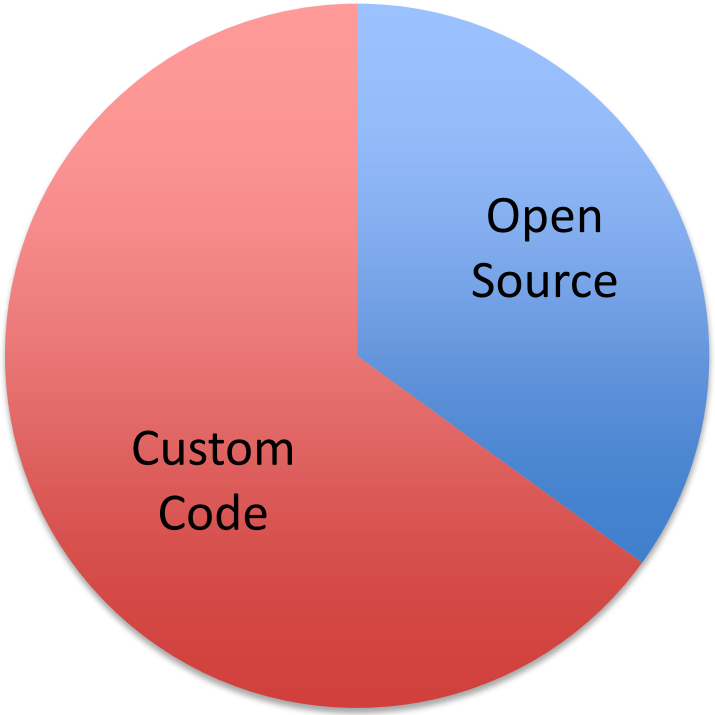

Mobility Computing

출처 : AhnLab

Open Source Software 사용 증가

오픈 소스 사용

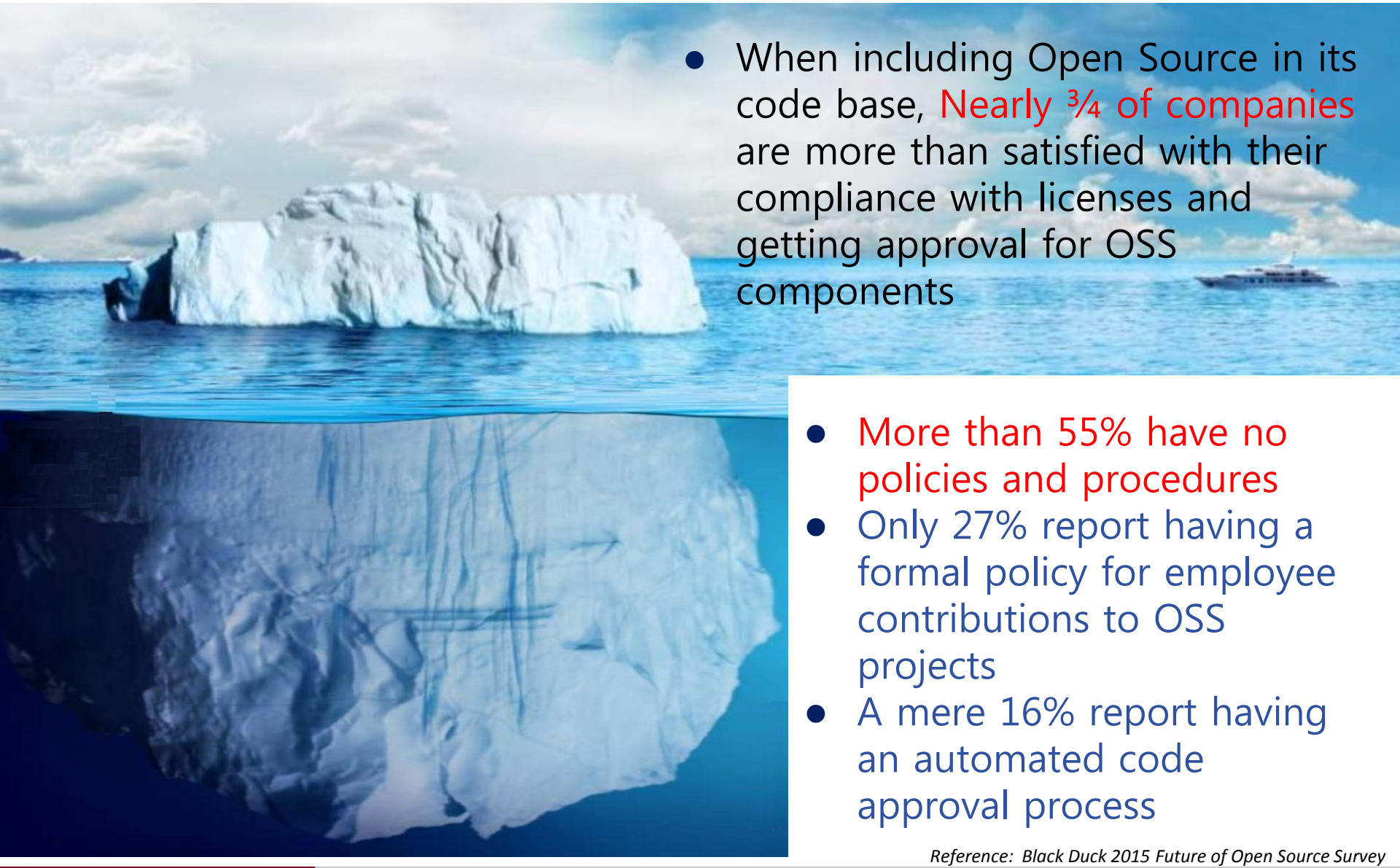
Composition of software tested across 1400 Black Duck customers



- 78% of companies run on open source
- Less than 3% don't use OSS in any way
- On average, open source comprised over 30% of the code base

Reference: Black Duck 2015 Future of Open Source Survey

오픈 소스 사용 정책



- When including Open Source in its code base, Nearly ¾ of companies are more than satisfied with their compliance with licenses and getting approval for OSS components

- More than 55% have no policies and procedures
- Only 27% report having a formal policy for employee contributions to OSS projects
- A mere 16% report having an automated code approval process

Reference: Black Duck 2015 Future of Open Source Survey

오픈 소스와 보안

- **오픈소스는 소스가 공개되어 보안에 취약하다?**
  - 많은 개발자들이 관여하여 상대적으로 안정적인 것은 사실
  - 공격자가 취약점 찾을 때도 유리하지만 해결책도 빠르게 제공됨
  - 그래도 보안에 투자해야 한다

- **모두가 문제가 아니라, 제대로 하고 있지 않은 곳이 있기 때문에 문제이다**
  - 그래서 보안에 투자해야 한다

오픈 소스와 보안 문제

- OSS 사용에 대한 정책이 없음
- 당연히, OSS 사용에 대한 절차도 없음
- 심지어, 개발자가 OSS사용을 부인하는 경우도 발생함
- 결국, Open Source가 어디에, 어떤 제품에, 얼마나 포함되었는지 관리가 되고 있지 않음

- Open Source에 취약점이 발견되었다고 해도 관심 없음
- 취약점이 개선되어도 어떻게 자기 제품에 적용할 지 모르거나 시간이 오래 걸림
- Third Party제품은 발견된 취약점과 관련이 있는지 확인조차 불가능함
- 취약점이 존재하는 오픈소스 소프트웨어가 아무런 주의없이 계속 사용되고 있음
- 결국, 발견된 취약점조차도 개선되지 않은(못한) 채로 운영되고 있는 실정임

오픈 소스와 보안 Survey

- 46% give OSS first consideration among security technologies
- 55% said Open Source delivers superior security
- However, 67% don't monitor Open Source Code for security vulnerabilities

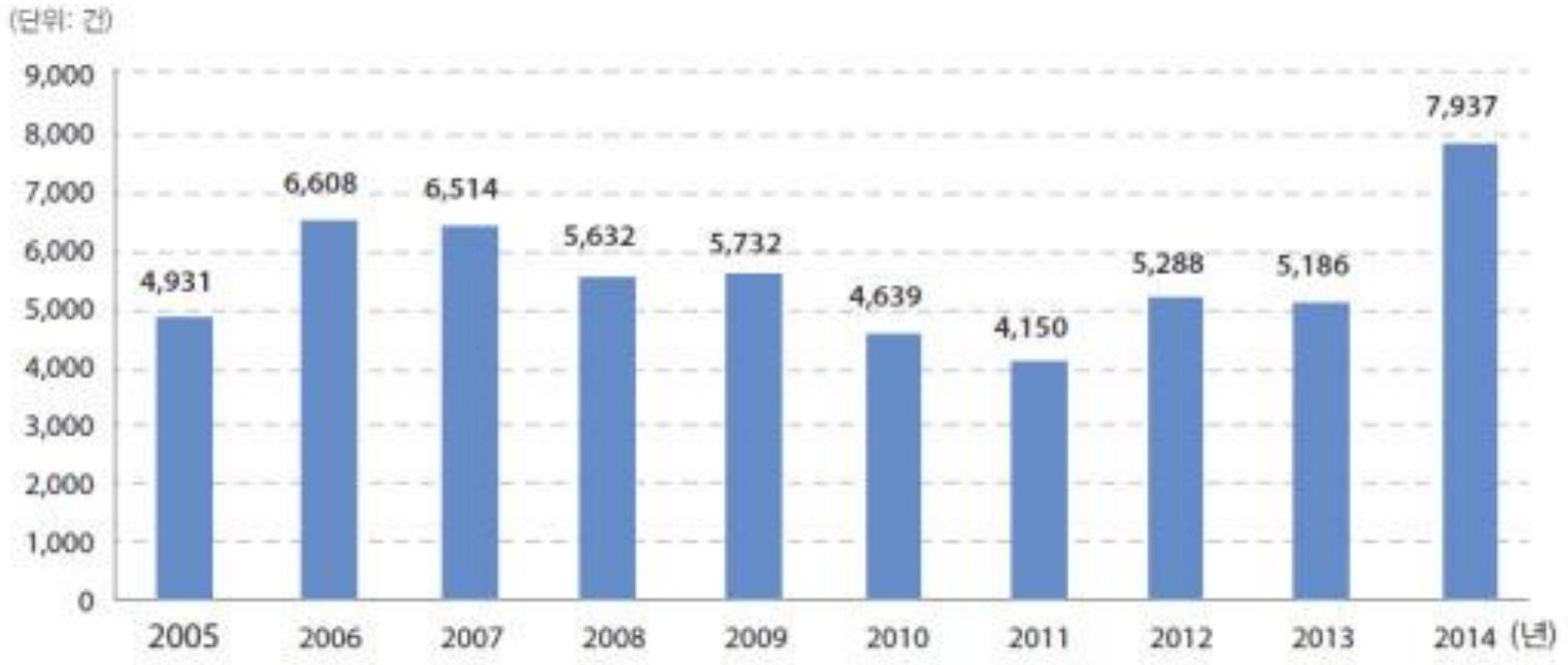
4000+ open source **vulnerabilities** are reported each year.

98% of companies are **unaware** of the open source code they are using.

67% of companies **don't monitor** their open source code for **security vulnerabilities.**

Reference: Black Duck 2015 Future of Open Source Survey

취약점

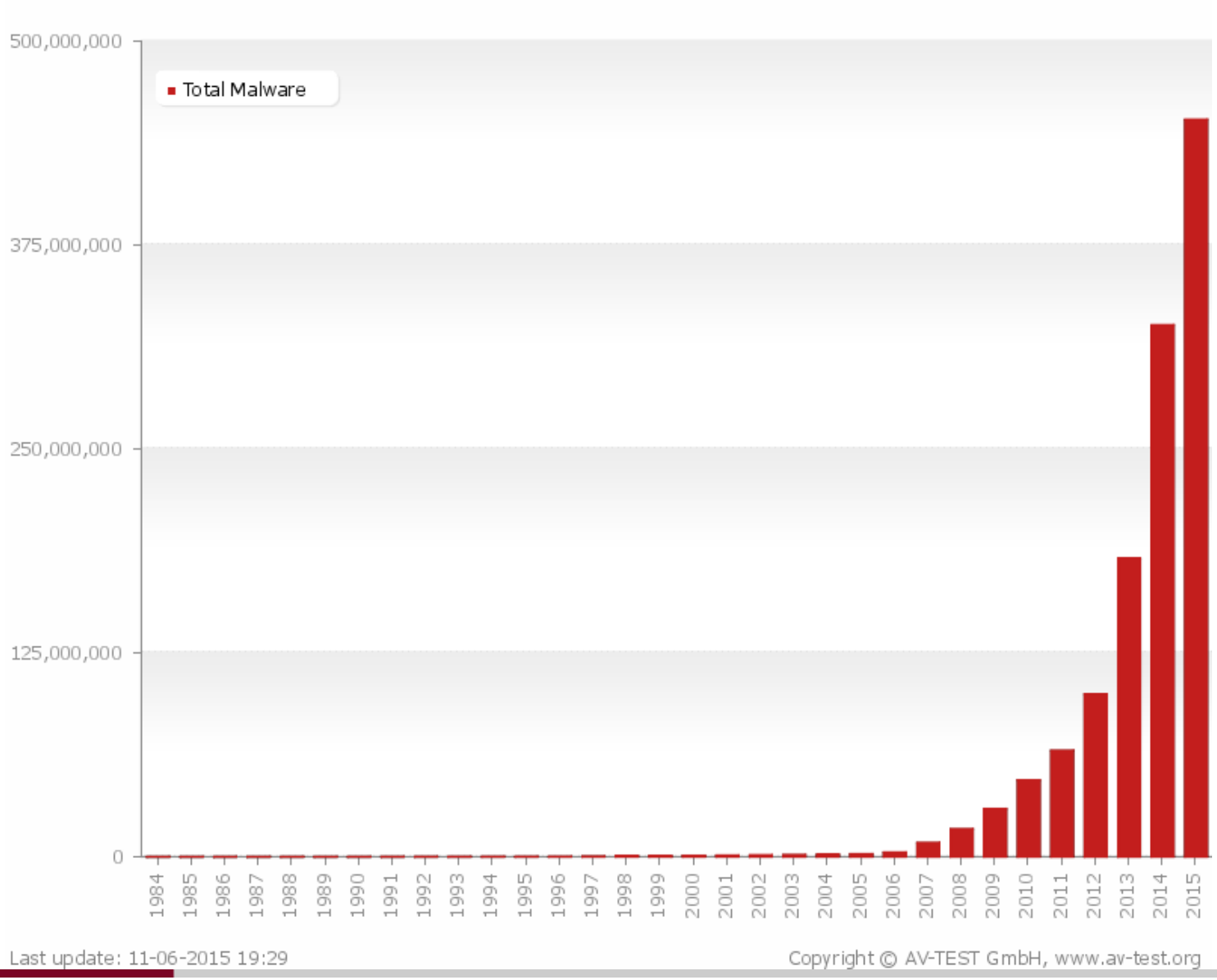


최근 10년간 CVE 취약점 공개 추이(출처 : 2015 국가정보보호백서) (http://www.cve.mitre.org)

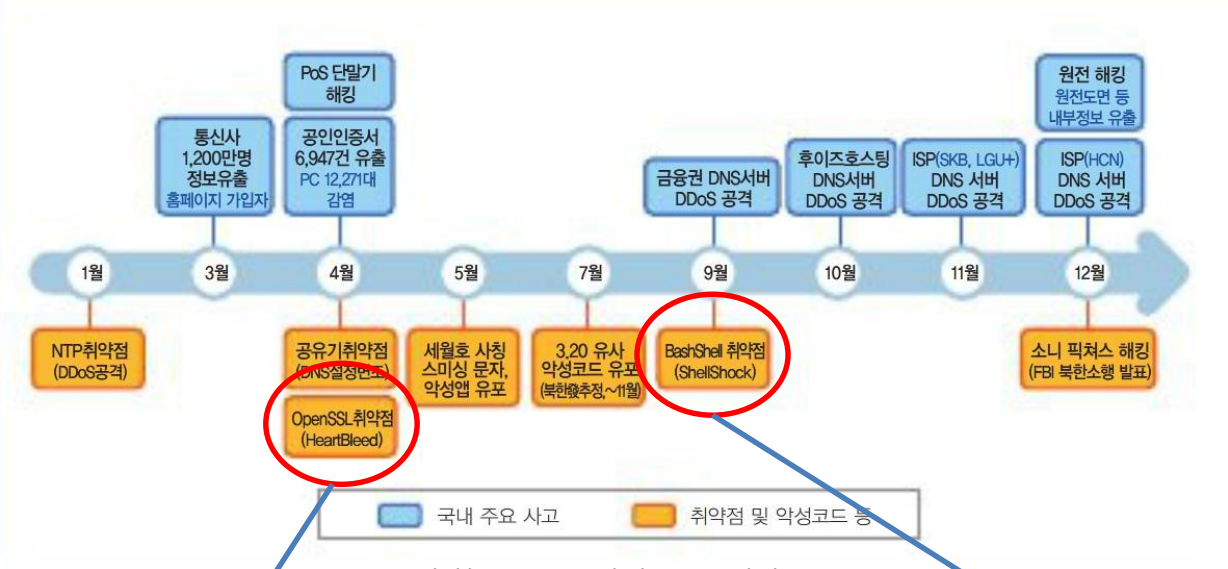
2014년

- 7,937개의 새로운 취약점 발견
- 그 중 약4,300개 정도가 오픈 소스
  - 오픈 소스의 사용은 증가 추세
  - 공격자도 분석을 위해 오픈 소스에 접근이 가능함
  - 새로운 취약점이 발견되면 Exploit형태도 함께 공개됨

Malicious Code



2014년 국내 주요 침해 사고



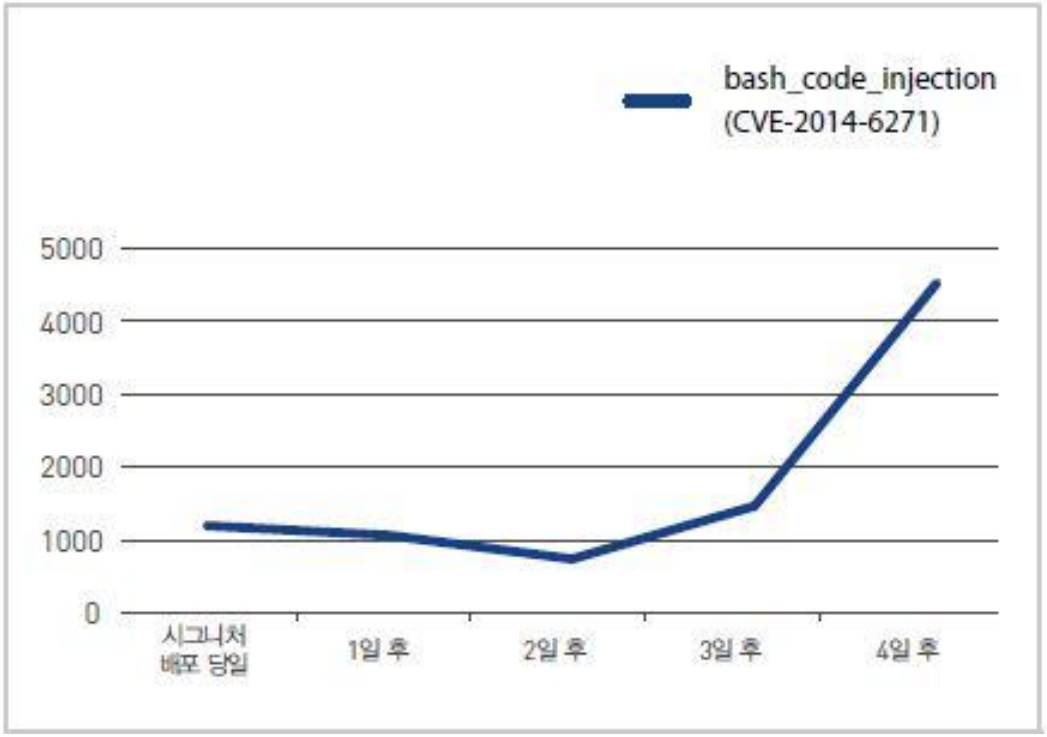
출처 : 2015 국가정보보호백서

- **Heartbleed**
  - 웹 서버와 브라우저 간의 안전한 통신에 사용하는 OpenSSL 라이브러리에서 나타난 버그
  - 2014년 4월에 발견
  - 비밀키 등 민감한 정보가 유출될 수 있음
  - 전 세계 50만대 시스템이 이 취약점에 노출됨. 아직도 20만대 이상의 장비가 취약한 상태에 있는 것으로 추정됨

- **Shellshock**
  - "bash" 쉘과 인터프리터에 있는 취약점
  - 웹사이트와 외부에 연결된 서버에서 악성코드를 원격으로 실행할 수 있는 취약점
  - 많은 웹사이트가 Open Source인 아파치 서버를 실행할 때 표준 CGI(Common gateway interface)로 bash를 사용하기 때문에 이 위협은 심각하고 널리 퍼졌음

2014년 9월 Bash코드 인젝션 취약점 탐지건수 추이

트러스가드 시그니처 명	당일	1일 후	2일 후	3일 후	4일 후
bash_code_injection (CVE-2014-6271)	1109	1069	625	1394	4529



출처 : AhnLab Threat Analysis

Regions affected by Shellshock

Asia	33.89%
Europe	33.77%
North America	10.59%
South America	7.66%
Oceania	2.12%
Africa	0.87%
Others	11.10%

2014년 9월~10월 Regions affected by Shellshock,

Asia	45.79%
Europe	22.54%
North America	13.64%
South America	7.71%
Oceania	6.41%
Africa	1.54%
Others	2.37%

2015년 8월~9월 Regions affected by Shellshock,

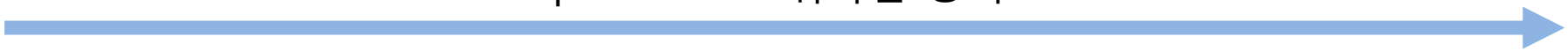
출처 : TrendMicro TrendLabs SECURITY INTELLIGENCE Blog

오픈 소스 주요 취약점

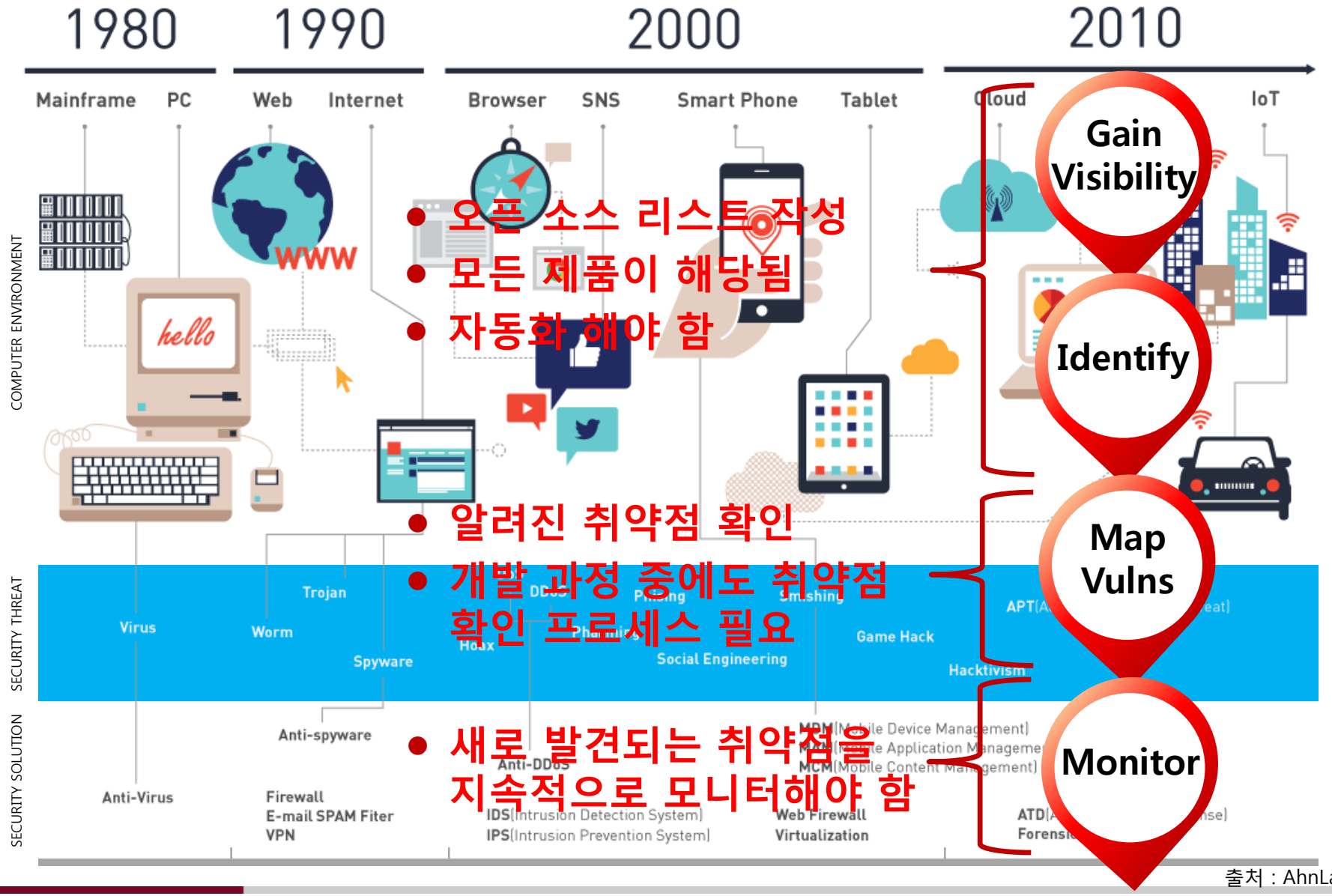
	Heartbleed	Shellshock	Freak	Ghost	Venom
배포시점	2011	1989	1990년대	2000	2004
발견시점	2014	2014	2015	2015	2015
Component	OpenSSL	Bash	OpenSSL	GNU C Library	QEMU

- **특 징**
  - 널리 사용되는 오픈 소스 Component에 있는 취약점임
  - 몇 년 동안 발견되지 않은 채로 정적/동적 도구를 이용하여 테스트된 제품에 존재
  - 불행하게도 SAST/DAST의 자동화된 툴보다 수동으로 Code Review를 하는 보안 연구자들 의해 발견됨

Open Source 취약점 증가



컴퓨터 환경과 보안의 발전



- 오픈 소스 리스트 작성
- 모든 제품이 해당됨
- 자동화 해야 함

- 알려진 취약점 확인
- 개발 과정 중에도 취약점 확인 프로세스 필요

- 새로 발견되는 취약점을 지속적으로 모니터해야 함

출처 : AhnLab

시사점

- **오픈 소스의 사용은 증가**
- **오픈 소스에 대한 취약점도 증가**

- **오픈 소스 보안에 대한 조직 내 소통 필요**
- **오픈 소스 사용 정책 및 프로세스 정립**
- **오픈 소스에 대한 가시성 확보는 필수**
  - 오픈 소스 코드 관리의 자동화 : 오픈 소스 코드의 분류와 추적
  - 오픈 소스 코드 리스트 작성 : 각 제품에 사용된 오픈 소스
  - 외주 용역 제품도 반드시 확인 : 오픈 소스 리스트 공개 및 안정성 보장 필요

- **오픈 소스 보안도 주기적이고 지속적인 보안 인식 개선과 교육 필요**

Thank you!!

Q & A

오픈소스와 보안

서울여자대학교 정보보호학과
조시행(sihaeng.cho@gmail.com)