

Security Boot Manager

TNTeam 팀

발표자 : 강호용

CONTENTS



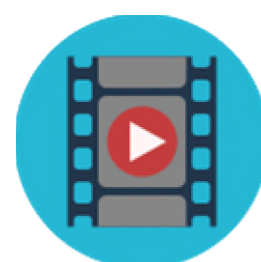
기획배경



개발내용



기대효과



시연 & 질의응답

IT기기 절도 매년 증가

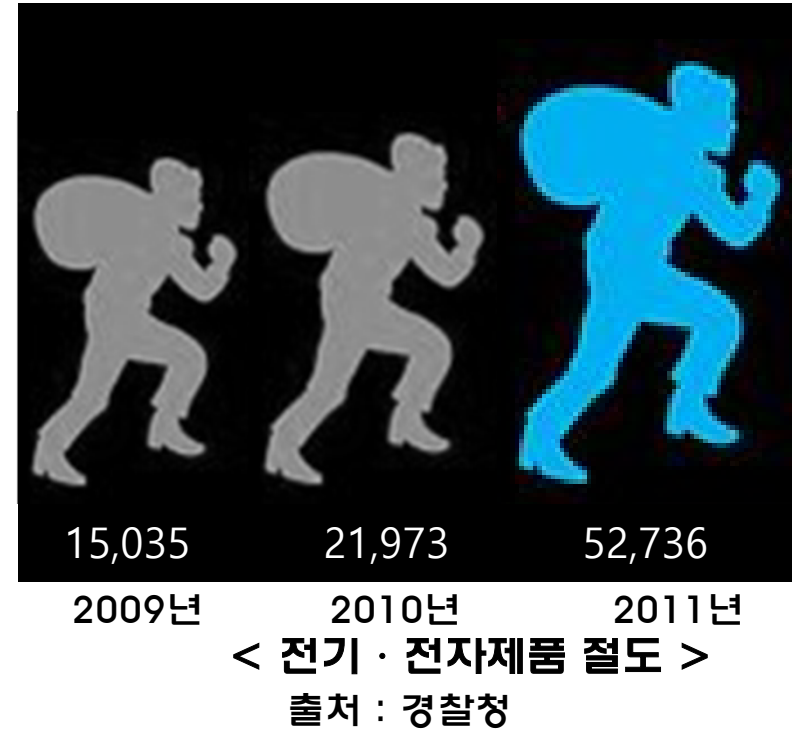
1

▶▶ 기획배경

▶ 개발내용

▶ 기대효과

▶ 시연 및 Q&A



- 현재 휴대폰이나 노트북과 같은 훔치기 용이한 IT기기 절도가 증가하고 있다.
- 부팅 정보를 상세하게 얻을 수 있는 라이브러리나 Framework 는 왜 없을까 ?

1

Q. 물리적 보안 장치 및 SW 보안 장치 문제점

▶▶ 기획배경

▶ 개발내용

▶ 기대효과

▶ 시연 및
Q&A



- 물리적 보안 장치는 비용이 발생할 뿐만 아니라 범인을 잡아낼 수 없다.
- SW적 보안 장치는 운영체제 로드 이후 작동되기 때문에
" 안전모드 부팅 등 빠져나갈 수 있는 방법들이 다수 존재한다. "

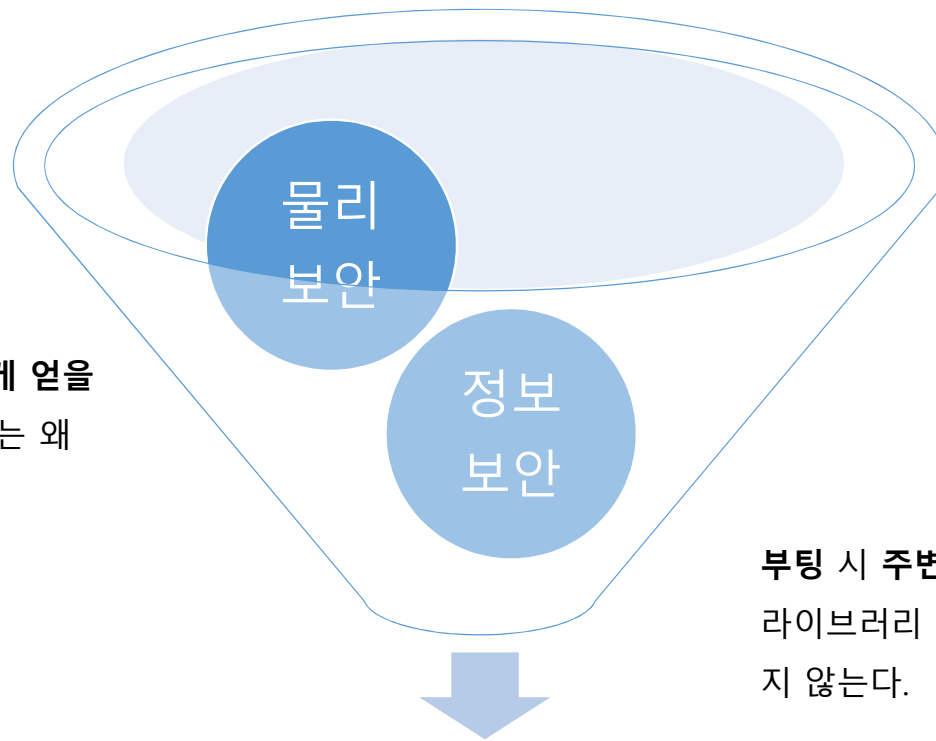
1

▶▶ 기획배경

▶ 개발내용

▶ 기대효과

▶ 시연 및 Q&A



부팅 정보를 상세하게 얻을 수 있는 Framework는 왜 없을까?

부팅 시 주변 환경 정보를 얻을 수 있는 라이브러리 혹은 프레임워크가 존재하지 않는다.

융합 보안

물리적으로 PC를 다시 되찾을 뿐만 아니라 부팅 정보를 상세하게 얻을 수 있는 Framework 필요!

그 결과 우리는 부팅 시 주변 환경 정보를 얻을 수 있는 Framework 개발하였습니다.

Web을 통해 부팅정보(IP, AP ssid ,접속시간)를 상세하게 파악 가능하게 하였습니다.

2

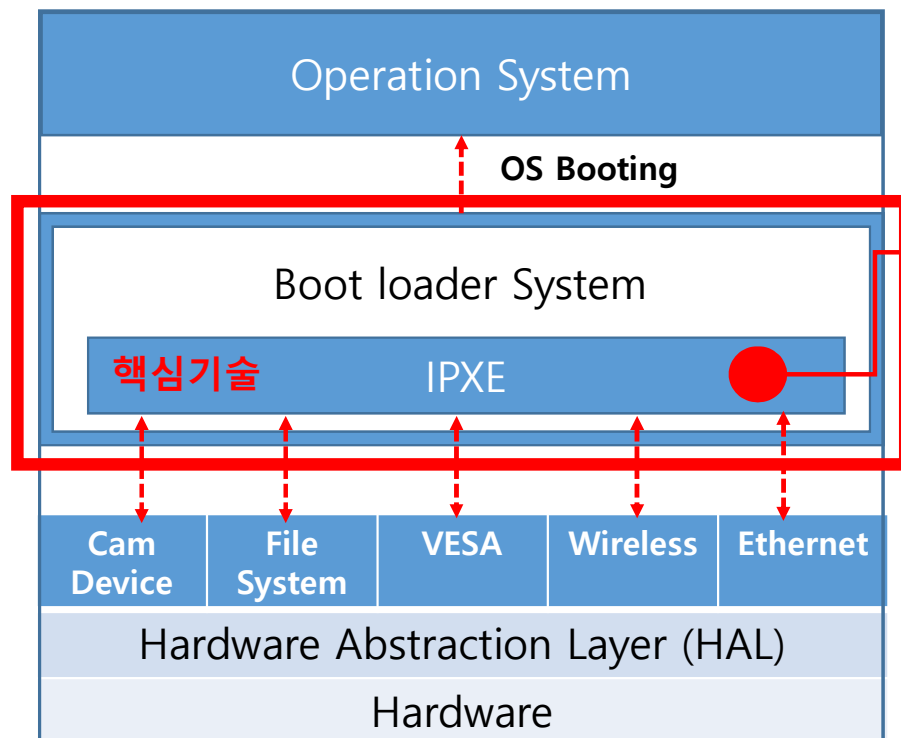
▶ 기획배경

▶▶ 개발내용

▶ 기대효과

▶ 시연 및 Q&A

시스템 구조



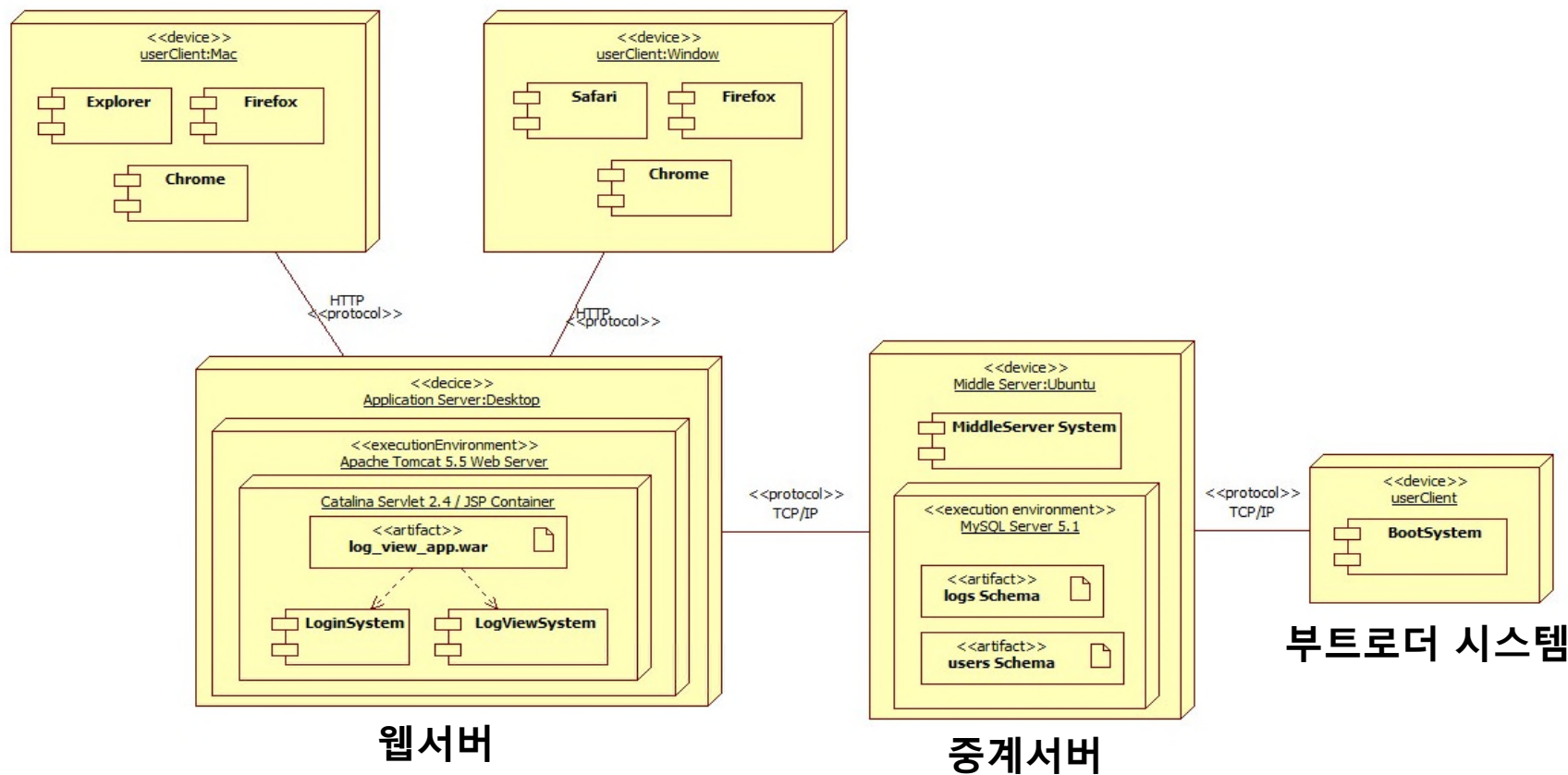
IPXE ?

부트 로드 단계에서 네트워크 연결하여 자료를 전송 할 수 있도록 해주는 오픈 펌웨어 시스템입니다.

이 기술을 이용하여 사용자 노트북 유/무선 체크 GUI환경, 무선 AP 리스트 출력, 주변 환경 Log 수집, 운영체제 커널로 제어 변경이 핵심 기술입니다.

2

시스템 구성도



▶ 기획배경

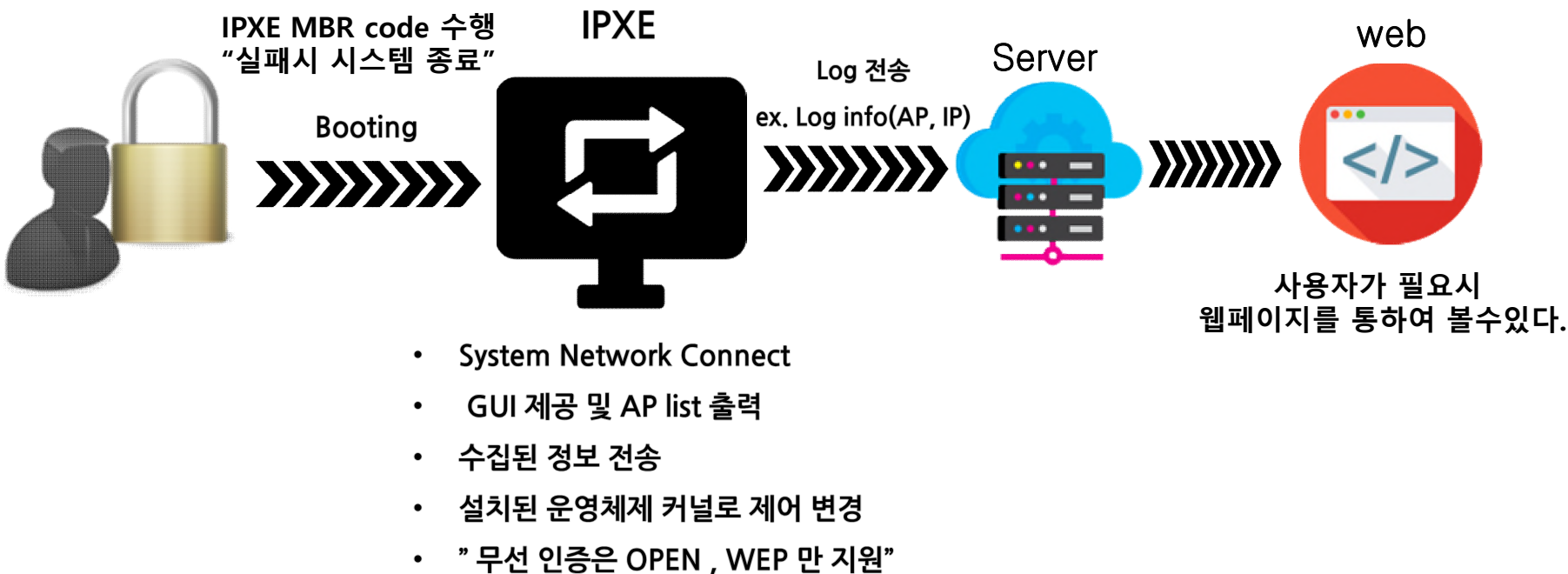
▶▶ 개발내용

▶ 기대효과

▶ 시연 및 Q&A

2

프로그램 동작흐름



▶ 기획배경

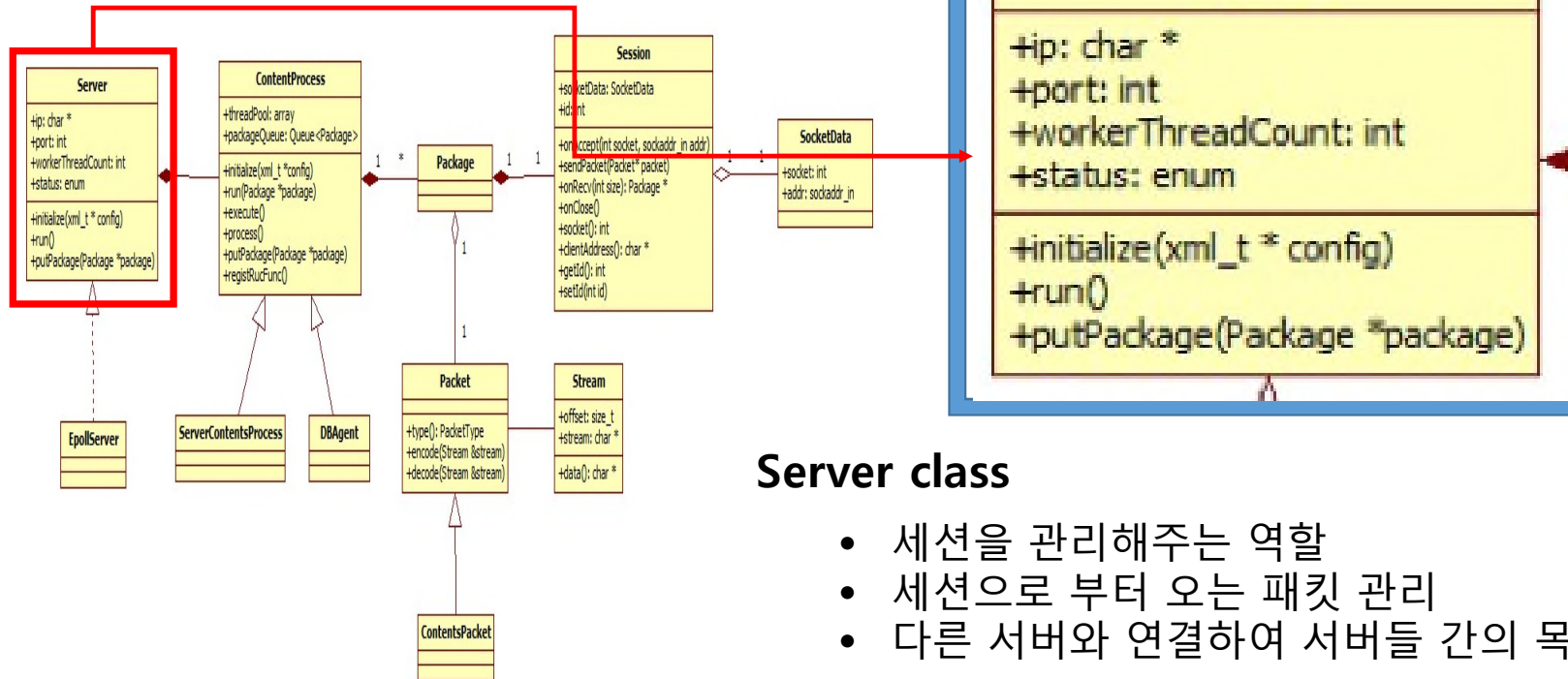
▶▶ 개발내용

▶ 기대효과

▶ 시연 및
Q&A

2

시스템 설계도 (#1 Middle Server)



▶ 기획배경

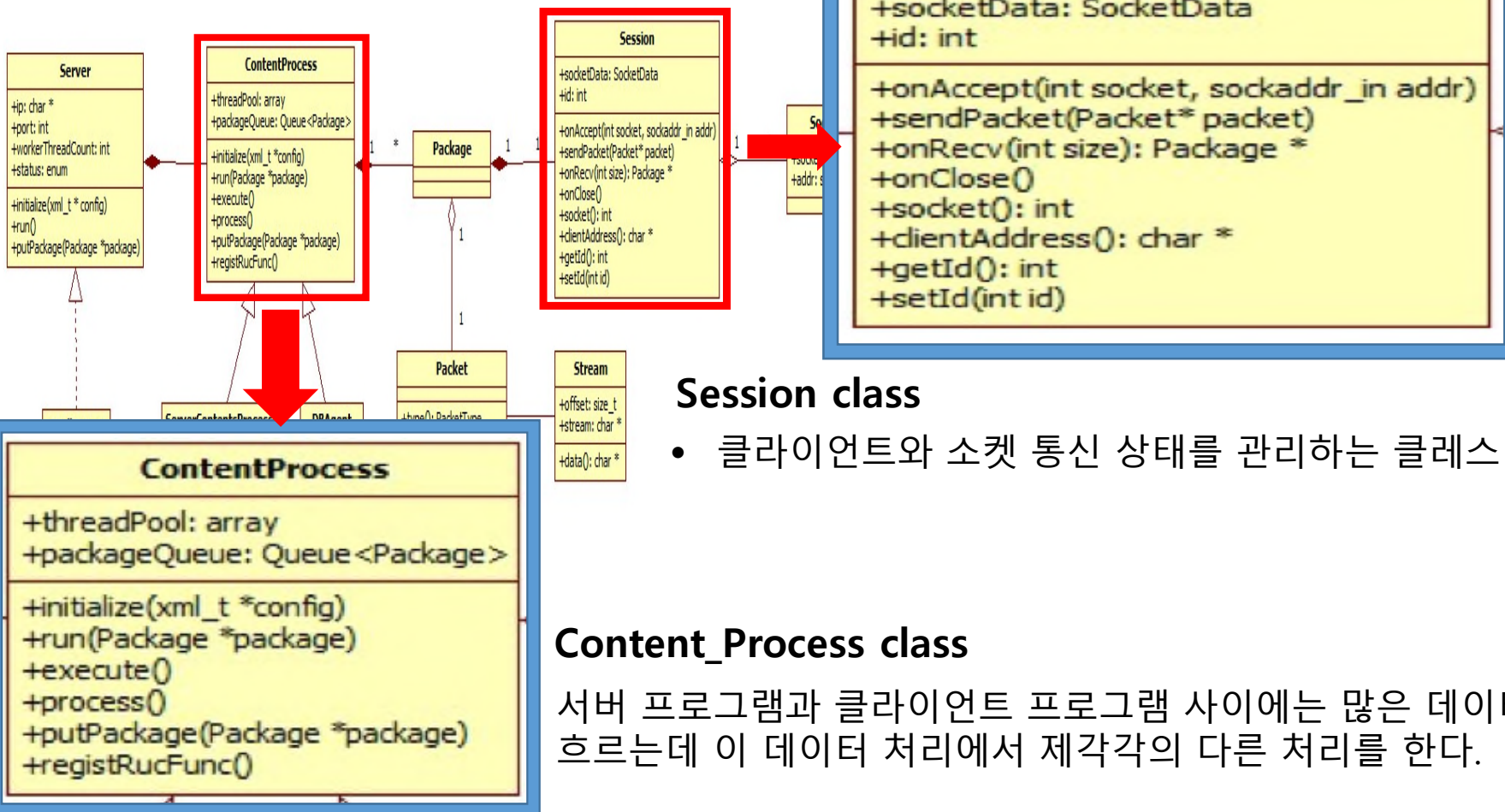
▶▶ 개발내용

▶ 기대효과

▶ 시연 및 Q&A

2

시스템 설계도 (#1 Middle Server)



▶ 기획배경

▶▶ 개발내용

▶ 기대효과

▶ 시연 및 Q&A

2

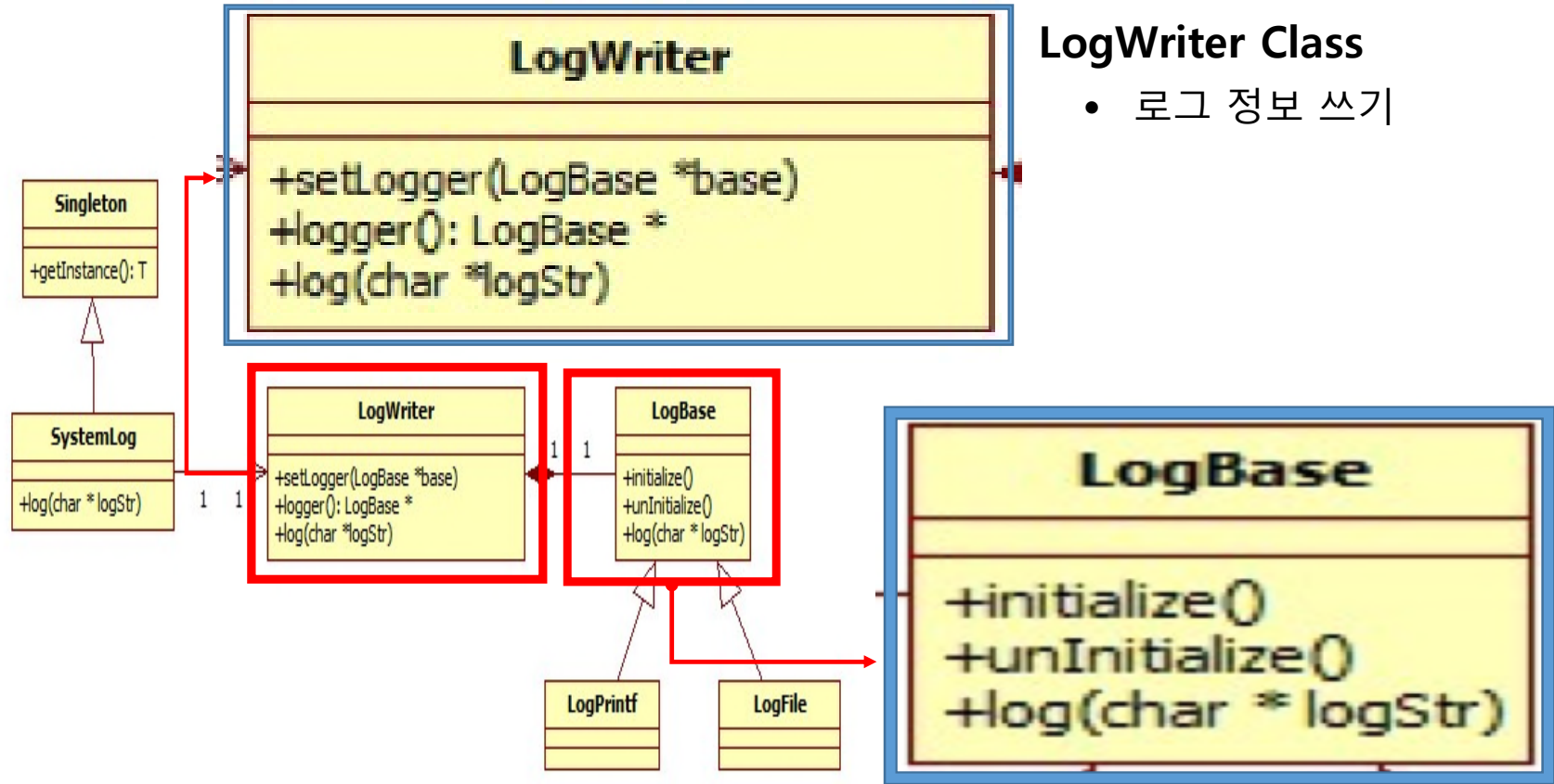
▶ 기획배경

▶▶ 개발내용

▶ 기대효과

▶ 시연 및 Q&A

시스템 설계도 (#1 Web Server)



LogWriter Class

- 로그 정보 쓰기

LogBase Class

- LogWrite를 상속한 클래스로 로그 정보를 출력하는 클래스

3

▶ 기획배경

▶ 개발내용

▶▶ 기대효과

▶ 시연 및
Q&A

시간적 효과

“각종 정보를 한번에 확인가능”

- 웹 사이트를 통한 AP ssid , ip , 접속시간 등을 한눈에 확인가능

“특정 운영체제 종속되어 동작하지 않고 커널 로드 되기전에 시행으로 빠른 성능 ”

- 커널 로드되기전 빠른 시행
Ex. 타 보안프로그램은 커널 로드 후 실행으로 인한 성능저하.

3

▶ 기획배경

▶ 개발내용

▶▶ 기대효과

▶ 시연 및
Q&A



효율적인 활용도

“사용자 패턴을 파악 가능 ”

ex. 사용자가 웹을 통하여 자신이 얼마나 컴퓨터를 사용하였는지 파악 가능

“설치 없이 사용 가능 ”

ex. 타 보안프로그램의 경우 특정운영체제 설치 필요

“특정 운영체제 종속되지 않는다. ”

ex. 타 보안프로그램의 경우 특정운영체제 종속되는 경우가 많다.

4

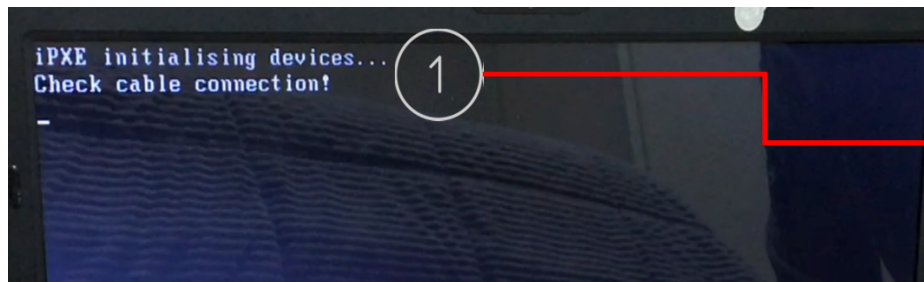
시연 시나리오 #1

▶ 기획배경

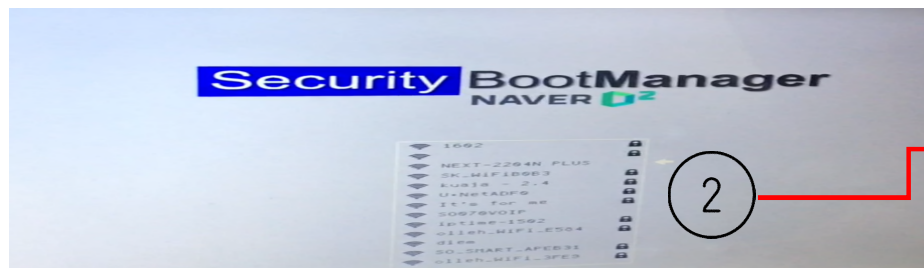
▶ 개발내용

▶ 기대효과

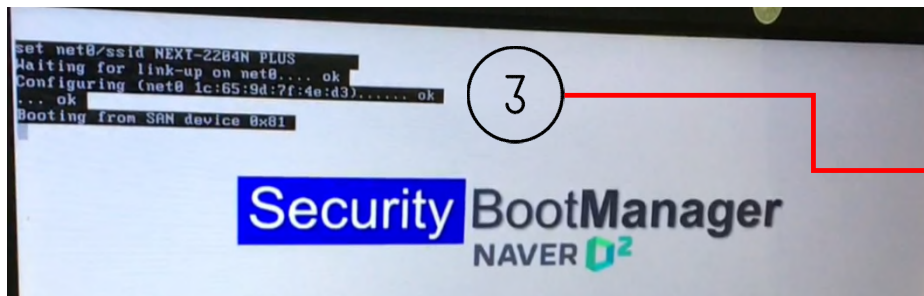
▶▶ 시연 및
Q&A



- IPXE devices 셋팅
- 연결 체크



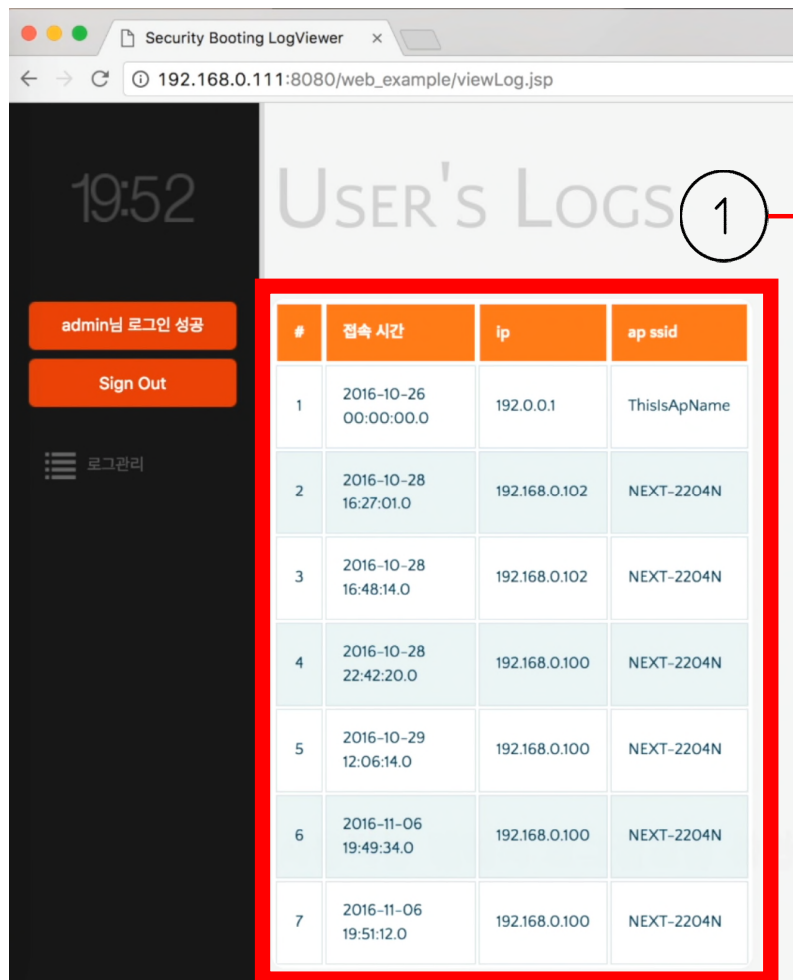
- GUI Display 출력
- AP리스트 출력
- 무선AP 선택가능



- 무선 AP연결 시도
- 수집된 Log정보를 전송
- 설치된 운영체제 커널로 제어 변경

4

시연 시나리오 #2



Security Booting LogViewer

192.168.0.111:8080/web_example/viewLog.jsp

19:52

USER'S LOGS

admin님 로그인 성공

Sign Out

로그관리

#	접속 시간	ip	ap ssid
1	2016-10-26 00:00:00.0	192.0.0.1	ThisIsApName
2	2016-10-28 16:27:01.0	192.168.0.102	NEXT-2204N
3	2016-10-28 16:48:14.0	192.168.0.102	NEXT-2204N
4	2016-10-28 22:42:20.0	192.168.0.100	NEXT-2204N
5	2016-10-29 12:06:14.0	192.168.0.100	NEXT-2204N
6	2016-11-06 19:49:34.0	192.168.0.100	NEXT-2204N
7	2016-11-06 19:51:12.0	192.168.0.100	NEXT-2204N

- 웹을 통하여 Log 정보 확인
- AP ssid, ip , 접속시간 확인가능

▶ 기획배경

▶ 개발내용

▶ 기대효과

▶▶ 시연 및 Q&A

4

▶ 기획배경

▶ 개발내용

▶ 기대효과

▶▶ 시연 및
Q&A

데모 영상

THANK YOU