「 K-사이버 시큐리티 챌린지 2019」 설명회

[정보보호 R&D 데이터 챌린지]

- AI기반 취약점 자동 탐지 트랙

손 경 아 주임

한국인터넷진흥원 보안기술확산팀

2019. 10. 1

Contents

1 트랙 개요

2 활용 데이터셋

3 결과물 제출 및 심사기준

4 예선 진행방식

5 본선 진행방식

6 예·본선 흐름도

7 시상내역

8 접수기간 및 신청절차

1. AI기반 취약점 자동 탐지 트랙 개요

개요

- 소프트웨어 바이너리의 취약점을 자동으로 탐지·패치·공격하는 기술의 성능을 검증하는 AI 해킹방어대회형 「AI기반 취약점 자동 탐지」 트랙 개최

세부 절차

01 신청 접수
- ✓ 신청서 접수 및 참가자격 확인

02 학습 데이터셋 배포
- ✓ 신청 접수 후 3~5일 이내에 메일로 배포
- ✓ 취약점 등 바이너리별 설명자료 배포

03 예선 진행
- ✓ 온라인 예선
- ✓ 탐지율 상위 7개 팀 본선진출

04 본선 진행
- ✓ 오프라인 본선
- ✓ 탐지율 및 발표심사

05 시상식 및 세미나
- ✓ 3개팀 시·포상
- ✓ 공개 세미나 개최

2. 활용 데이터셋

CWE 기반의 주요 취약점이 포함된 소프트웨어 바이너리 약 60개 활용

- **난이도는 상·중·하 로 구분하여 균등 분포, 학습 데이터셋 및 본선 데이터셋에 랜덤하게 배포**

※ 난이도 설정은 소스코드의 복잡도, 메모리 보호기법 적용 등을 기준으로 구분

학습 데이터셋

- ✓ (설명) CWE 기반 취약점이 포함된 바이너리셋
- ✓ (규모) 10개
- ✓ (구성) 바이너리 , 설명자료
  - 바이너리 동작 환경 : Linux 32bit
  - 설명자료 : 각 바이너리 별 취약점 정보, 소스코드, 적용된 메모리 보호기법, 난이도 분석 등 상세정보

예 · 본선 데이터셋

- ✓ (설명) CWE 기반의 취약점이 포함된 바이너리를 대회 시스템의 각 팀별 경연서버에서 실행
- ✓ (규모) 예선 20개, 본선 30개
- ✓ (구성) 라운드별 바이너리 실행
  - 라운드당 10개 바이너리 배포

2-1. 활용 데이터셋 – 취약점 항목

취약한 SW 바이너리 데이터셋 개발 과정에서 시스템 해킹과 관련된 CWE 주요 취약점 리스트 적용

※ CWE (Common Weakness Enumeration) : 수집된 소프트웨어 취약점의 정의, 설명 등 정식 목록 분류체계

1 CWE-120 : Buffer Overflow

Stack-based Buffer Overflow (CWE-121)

o 변수의 길이보다 더 긴 길이의 값을 변수에 write할 때 발생

```
#define BUFSIZE 256
int main(int argc, char **argv){
char buf[BUFSIZE];
strcpy(buf, argv[1]);
}
```

버퍼 크기는 고정되어 있지만, argv[1] 문자열이 크기를 초과하면 오버플로우 발생

Heap-based Buffer Overflow (CWE-122)

o malloc()과 같은 함수로 동적 할당한 메모리를 덮어 씀으로써 프로그램 함수 포인터를 조작하여 발생

```
#define BUFSIZE 256
int main(int argc, char **argv){
char *buf;
buf=(char*)malloc(sizeof(char)*
BUFSIZE);
strcpy(buf, argv[1]);
}
```

버퍼에는 고정 크기의 힙 메모리가 할당되지만, argv[1] 문자열이 크기를 초과하면 오버플로우 발생

2 CWE-134 : Format String Attack

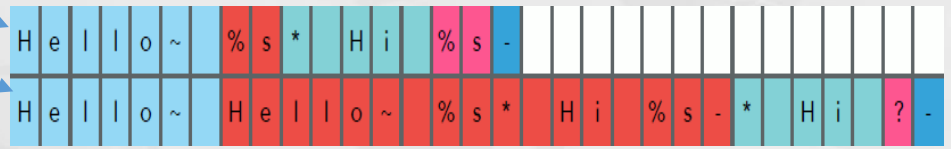
o Format String

- 어떠한 형식이나 형태를 지정해 주는 문자열
- 예) printf("Hello %s \ n", str);

o printf()와 포맷 스트링 작용

- 일반 문자열 : 그대로 출력
- 형식 지시자 : 지시자에 대한 내용을 스택에서 pop하여 출력

```
printf("%s", buf);  //① .....문자열 정상 출력
printf(buf);        //② .....취약한 형태
```



[CWE 항목 예시]

3. 결과물 제출 및 심사기준

1. KEY 파일	✓ 취약점을 공격하여 얻어낸 KEY 파일 제출 ✓ 취약점 바이너리의 난이도를 고려하여 제출한 **KEY 파일 점수** 부여 ✓ Key 파일 : 16byte의 16진수 문자열
2. 알고리즘 설명문서	✓ 취약점 자동 탐지 프로그램의 알고리즘 설명문서 제출 ✓ 기술 개요도 또는 프로그램 구성도, 예선 실행 결과, 보완점 등을 작성 ✓ 평가내역 : **자동화**, 알고리즘 **창의성** 평가 ※ 알고리즘 설명문서를 검토하여 편법 사용 등 문제 발견 시, 수상에서 제외될 수 있음
3. 발표자료	✓ 알고리즘 설명문서를 바탕으로 **15분 분량**으로 작성 ✓ 평가내역 : **자동화**, 알고리즘 **창의성** 등

최종 스코어 (80%) + 발표 점수 (20%)

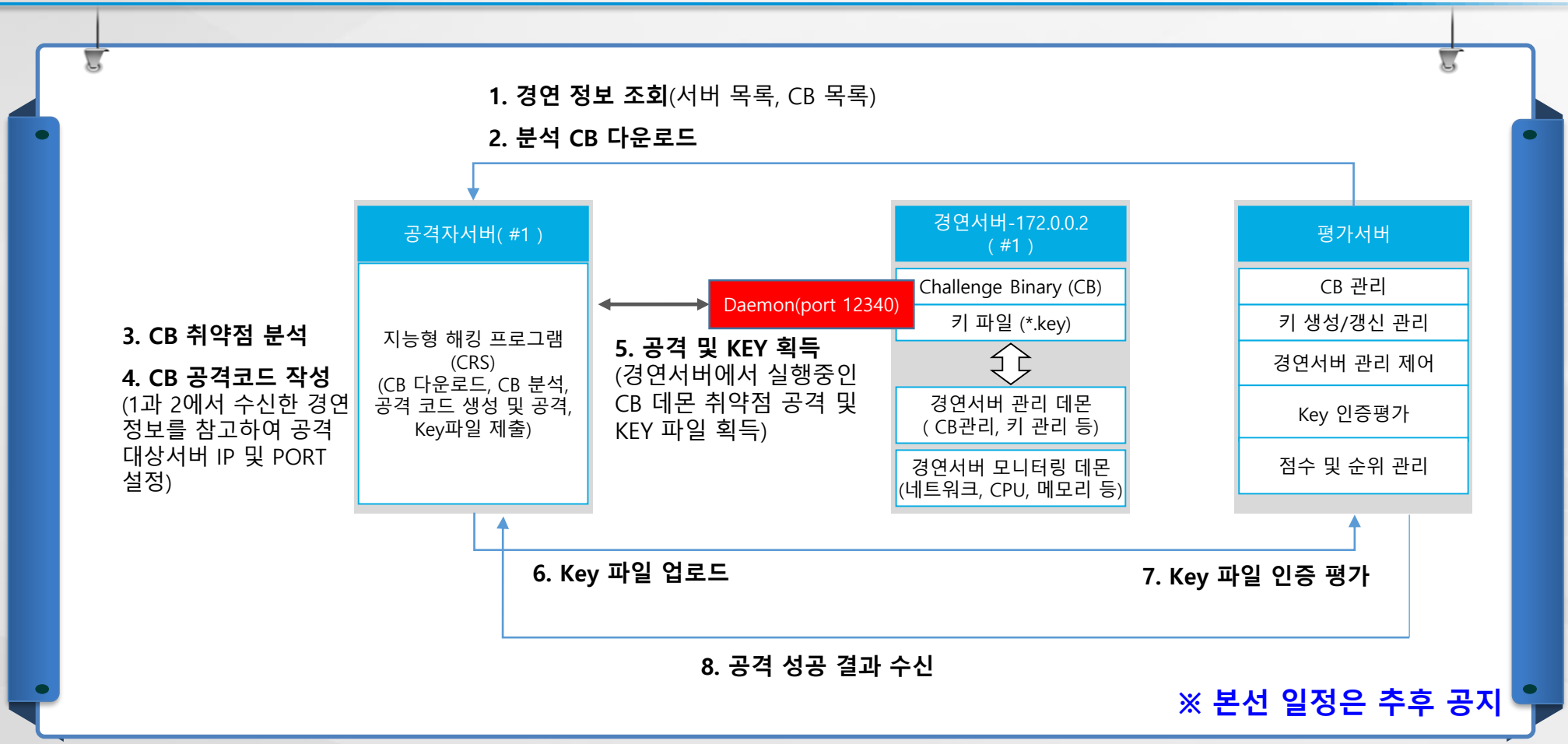
4. 예선 진행방식

- 11월 8일 10:00~18:00, 온라인 예선 진행
- 준비 라운드 : 11월 7일 10:00~18:00 (대회 서버 오픈, 테스트 가능)

- (일정) 11월 8일 10:00~18:00
- (1라운드) 공격·패치 / 약 15개 / 각 팀 별 바이너리 패치 후 상대팀 경연 서버 공격
  ※ 패치는 '2020년 해킹방어 대회' 개최 준비를 위한 시범 대회 형식으로 1라운드만 진행
- (2라운드) 공격 / 10개 / 각 팀의 경연 서버에 있는 바이너리 취약점 공격
- (3라운드) 공격 / 10개 / 각 팀의 경연 서버에 있는 바이너리 취약점 공격
- (심사기준) 탐지율 + 패치 점수
- (본선 진출팀) 상위 7개팀
- (서버 제공) 각 팀 별 경연 서버 1대, 공격 서버 1대 배포 (10월 14일 배포 예정)

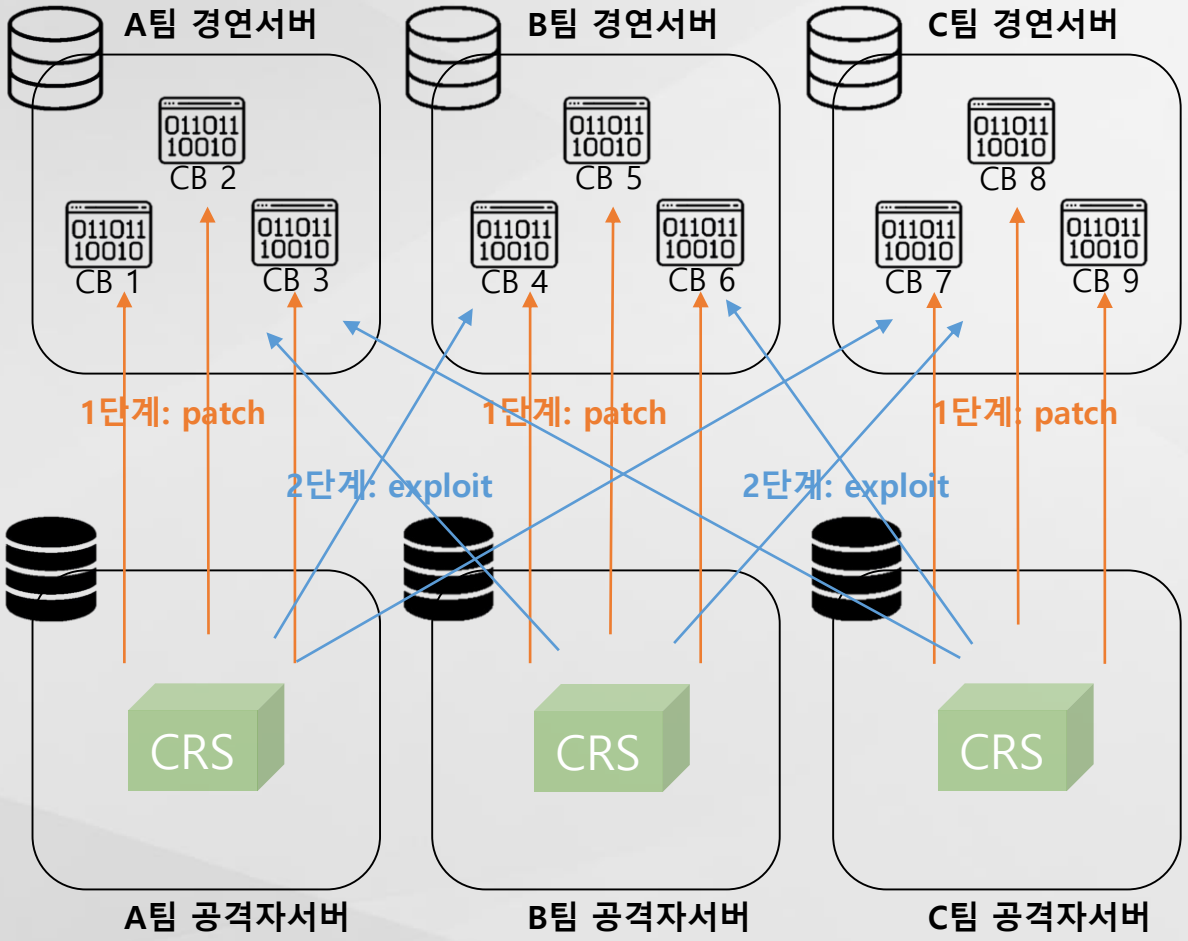
5. 본선 진행방식

- 11월 21~22일 예정, 오프라인 본선 진행 (발표 평가 포함)
- 준비 라운드 : 11월 20일 10:00~18:00 (대회 서버 오픈, 테스트 가능)

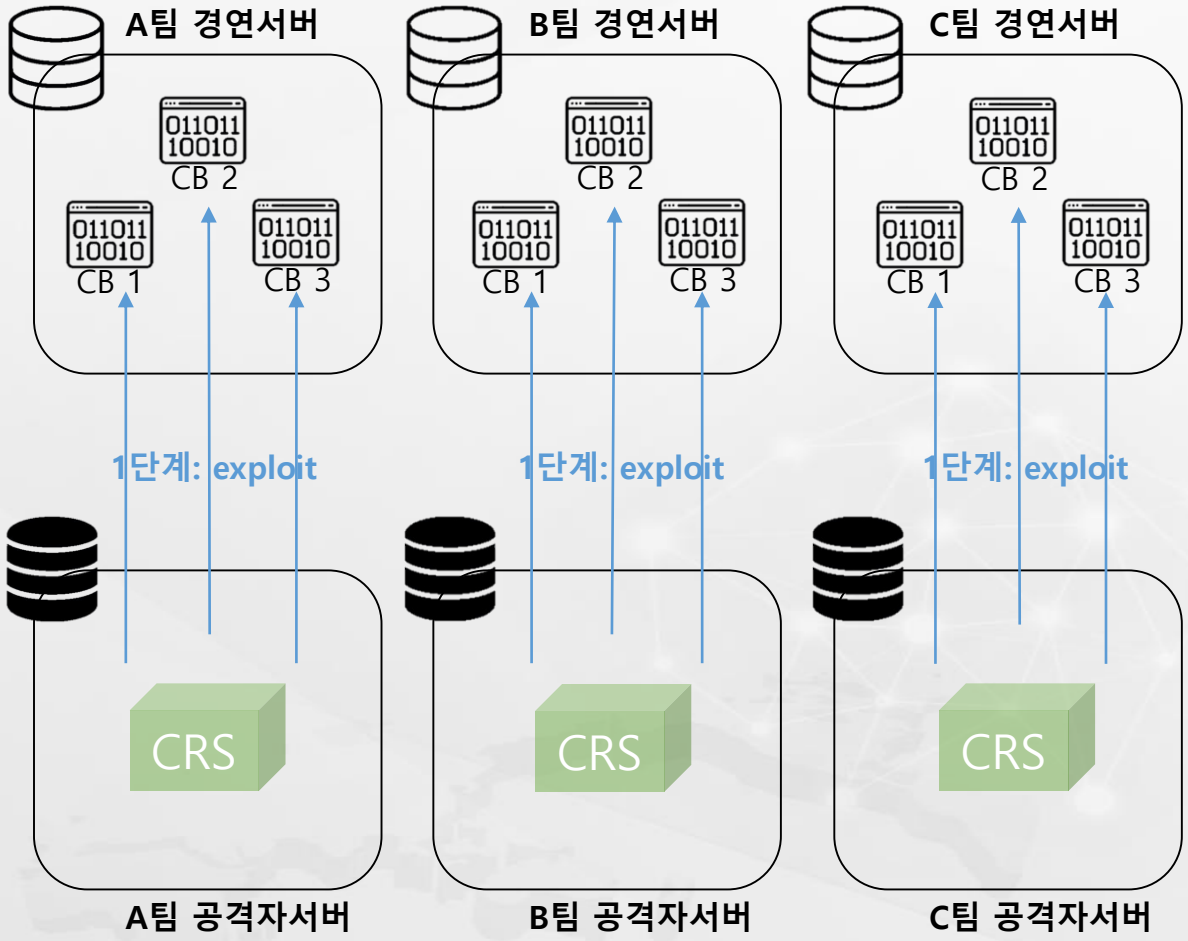


6. 예·본선 흐름도

패치 · 공격 (예선 1라운드)

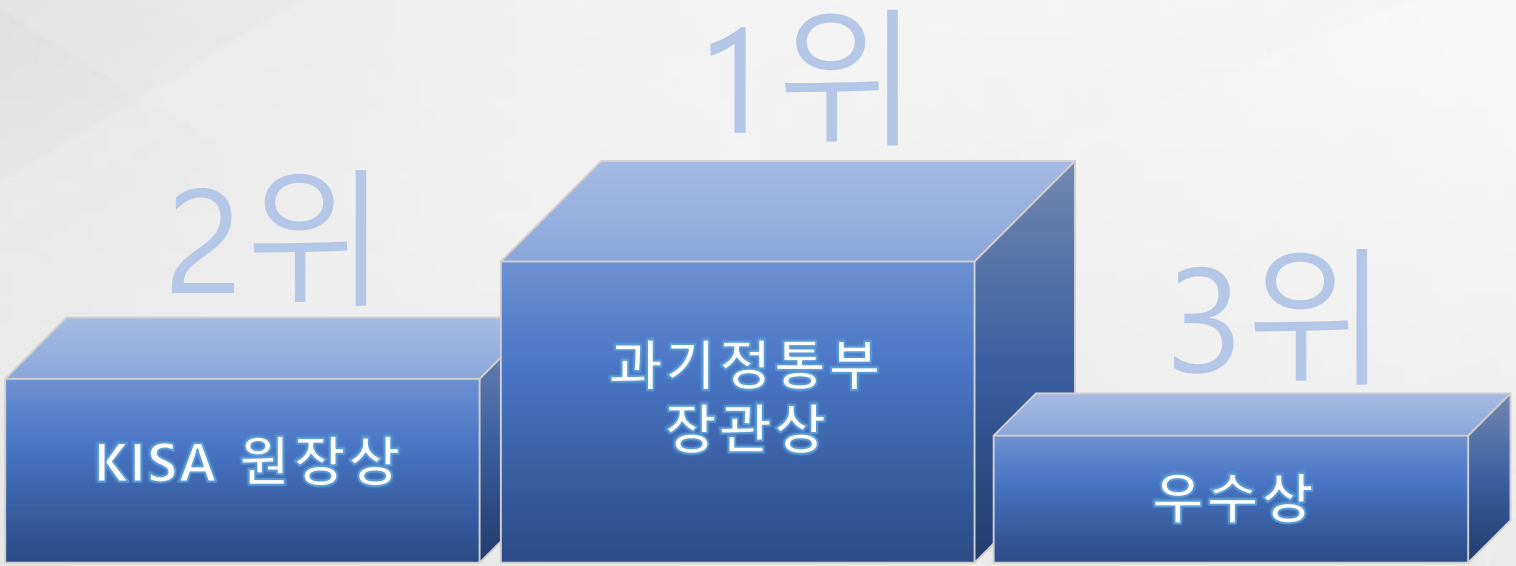


공격 (예선 2~3라운드, 본선 1~3라운드)



※ CB (Challenge Binary) : 취약점이 존재하는 바이너리
※ CRS (Cyber Reasoning System) : 참가자가 개발한 지능형 해킹방어 프로그램

7. 시상내역



8. 접수기간 및 신청절차

접수기간

2019.10.1(화) ~10.31(목)

신청절차

01 datachalleng.kr

- ✓ 정보보호 R&D 데이터챌린지 홈페이지 접속

02 「AI기반 취약점 자동 탐지 트랙」

- ✓ 트랙 선택

03 신청서류 다운 및 작성

- ✓ 참가신청서
- ✓ 약정서

04 rnd_dataset@kisa.or.kr로 제출

- ✓ 이메일로 신청서류, 소속증명서 제출

감사합니다.

<문의처>
한국인터넷진흥원 손경아 주임
(T. 061-820-1256)
(E. rnd_dataset@kisa.or.kr)