

IoT 취약점 탐지 자동화 MAgic Fuzzer

한양대학교 ICEWALL 조성준, 정재영, 김창현

목차

Background

- IoT
- CGI
- 취약점 탐지/분석 방법
- MAgIC Fuzzer의 필요성

MAgIC Fuzzer

- Wrapper Generation
- Seed Generation

Conclusion

- MAgIC Fuzzer의 가치
- 프로젝트 성과

Internet of Things

 [블록체인 IoT 플랫폼 젠서, 비트코인캐시와 파트너십](#) 아이뉴스24 | 4시간 전 | 네이버뉴스 |

제닉스 스튜디오는 블록체인 기반 사물인터넷(IoT) 플랫폼 젠서(xensor)가 비트코인 캐시(BCH)와 파트너십을... IoT 플랫폼 젠서는 번거로운 관리포인트들을 자동화하여 데이터를 축적하고 거래할 수 있으며, 저렴한...

- ▶ [블록체인 기반 IoT 플랫폼 젠서, 비트코인 ...](#) 데일리시큐 | 2시간 전
- ▶ [블록체인 기반 IoT 플랫폼 젠서, '비트코인 ...](#) 헬로티 | 5시간 전
- ▶ [블록체인 기반 IoT 플랫폼 '젠서', 비트코인 ...](#) 데이터넷 | 8시간 전
- ▶ [블록체인 기반 IoT 플랫폼 '젠서', '비트코인...](#) 청년일보 | 2시간 전

[관련뉴스 9건 전체보기 >](#)

 [경기도시공사, 매입임대주택 IoT모니터링 시스템 구축](#) 스포츠서울 | 1일 전 | 네이버뉴스 |

경기도시공사, 매입임대주택의 독거노인 및 장애인 세대 등 안전취약계층을 대상으로 IoT모니터링 시스템을... 28일 공사에 따르면 스마트 전기안전서비스란 일반적인 안전점검에 더해 한국전기안전공사의 IoT모니터링...

- ▶ [경기도시공사, IoT로 취약계층 전기재해 예...](#) 뉴스1 | 1일
- ▶ [IoT로 취약계층 전기재해 사전 예방](#) 기호일보 | 21시간 전

 ["IoT, HW-SW 보안 만으로는 부족하다"](#) 전자신문 | 11면2단 | 3일 전 | 네이버뉴스 |

오염, IoT를 통한 네트워크 공격 등 다양한 분야로 확장 가능하다고 지적했다. 켈리 CTO는 “인슐린 펌프를 조절하는 의료기기가 해킹을 당하게 되면 이는 곧바로 우리 생명을 위협하는 끔찍한 결과를 낳게 된다”면서...

 ["IoT기기 해킹 불안하면 무료점검 받으세요"](#) 아이뉴스24 PICK | 2019.10.27. | 네이버뉴스 |

최근에는 이를 악용해 IoT 기기를 해킹하는 사례가 늘고 있지만, 본래 인터넷에 접속된 기기를 파악하기 위한 목적으로 만들어진 정보공유 사이트다. KISA는 쇼단에서 아이디어를 얻어 지난해부터 IoT 취약점 점검...

- ▶ [늘어나는 IoT 기기 해킹…KISA, “무료로 점...](#) 디지털데일리 | 2019.10.27. | 네이버뉴스
- ▶ [IoT 기기 취약점 점검 시행될까](#) ZDNet Korea PICK | 2019.10.27. | 네이버뉴스
- ▶ [KISA, IoT 취약점 점검 서비스 시작](#) 데이터넷 | 2019.10.27.
- ▶ [일본은 법으로 허용…한국은 규제에 막혀](#) 헤럴드경제 | 2019.10.27. | 네이버뉴스

[관련뉴스 5건 전체보기 >](#)

Internet of Things

	<p>시스코 2911/K9 최저 1,596,600원 판매처 9</p>		<p>시스코 1921-SEC/K9 최저 1,349,100원 판매처 2</p>		<p>RN214 최저 480,000원 ① 팔고 넷기어 판매처 210 랜섬웨어 방지</p>		<p>RN422 최저 620,000원 ① 팔고 넷기어 판매처 213 랜섬웨어 방지</p>
	<p>Cisco 라우터/기가비트 WAN VPN / ... 343,300원 인터넷파크 N Pay</p>		<p>해외 Cisco라우터 Cisco 880 Series Int... 948,420원 옵션</p>		<p>시놀로지 DS218+ 최저 436,000원 판매처 635 ★ 4.8 (999+) 쪽 185</p>		<p>EFM네트웍스 아이피타입 NAS2 Dual 최저 164,860원 판매처 1,145 ★ 4.7 (820) 쪽 112</p>
	<p>Cisco RV325 듀얼 기가비트 WAN VP... 581,690원 다다몰 N Pay</p>		<p>Cisco90시리즈 PCD SF90-24 206,420원 클릭DC N Pay</p>		<p>시놀로지 DS218J 최저 208,000원 판매처 722 ★ 4.8 (586) 쪽 133</p>		<p>시놀로지 DS918+ 최저 727,000원 판매처 642 ★ 4.8 (763) 쪽 69</p>

IoT 취약점의 금전적 가치

IoT

Google Home	\$25,000
Amazon Alexa	\$25,000
Apple Watch Series 4	\$25,000
Samsung Galaxy Watch	\$25,000

\$100,000

HITB Driven2Pwn

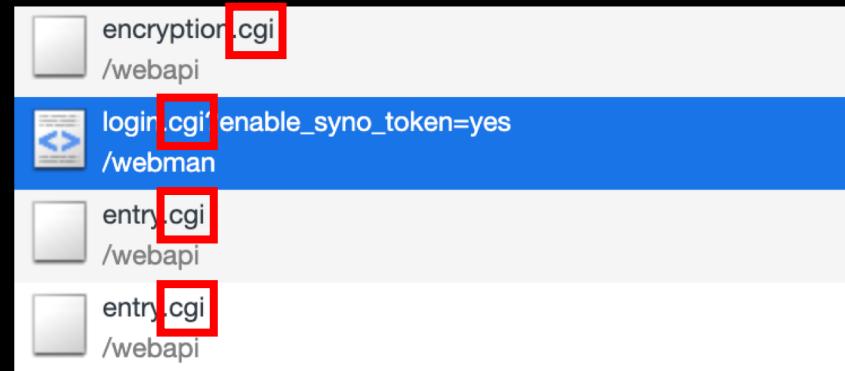
ZDI Target List

Eligible Router Brands

ASUS, Cisco, D-Link, Huawei, Linksys, MikroTik, Netgear, TP-Link, and Ubiquiti.

Common Gateway Interface

라우터, NAS, 프린터 등에서 사용하는 사용자 인터페이스



NAS 제품 (예시)

일반적인 취약점 탐지/분석 방법

Code Auditing

- 1. 소스코드가 있을 경우
- 2. 사람이 해야 함

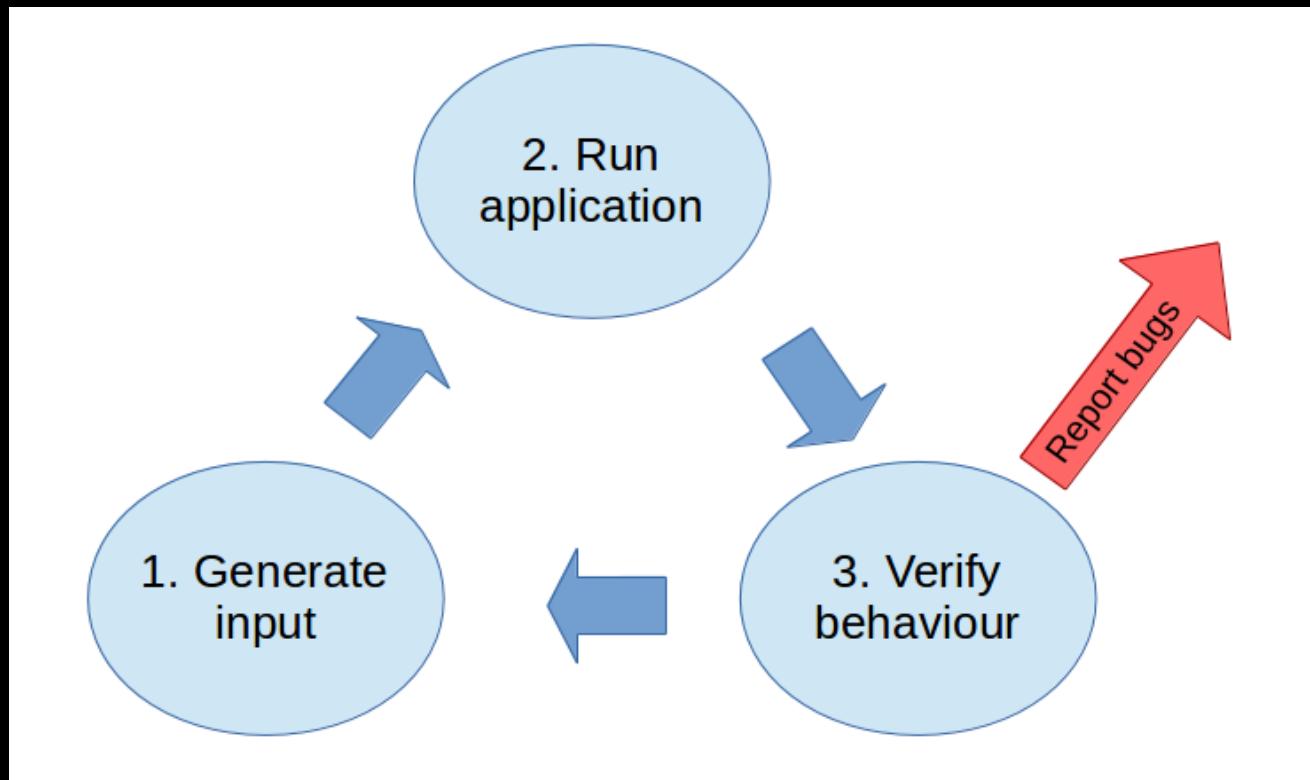
Reversing

- 1. 소스코드가 없을 경우
- 2. 사람이 해야 함

Fuzzing

- 1. 소스코드 유무 중요 X
- 2. 자동화 가능

Fuzzing



<http://9livesdata.com/wp-content/uploads/2018/03/1.png>

Fuzzing

```
1 #include <stdio.h>
2
3 int main() {
4     char buf[0x10];
5     gets(buf);
6     return 0;
7 }
```

```
→ Desktop ./test
warning: this program uses gets(), which is unsafe.
aaaa

→ Desktop ./test
warning: this program uses gets(), which is unsafe.
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
[1] 4775 abort      ./test
→ Desktop
→ Desktop
```

Fuzzing

```
1 #include <stdio.h>
2
3 int main() {
4     char buf[0x10];
5     gets(buf);
6 }
7 } 취약한 코드
```

```
→ Desktop ./test
warning: this program uses gets(), which is unsafe.
aaaa 정상 입력
```



```
→ Desktop ./test
warning: this program uses gets(), which is unsafe.
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa 비정상 입력
```

```
[1] 4775 abort      ./test
→ Desktop
→ Desktop
```

위 예시는 손 퍼징

위 과정을 자동화하면 퍼저.

기존에 공개된 Fuzzer

```
→ Desktop ./test
warning: this program uses gets(), which is unsafe.
aaaa
```

```
→ Desktop ./test
warning: this program uses gets(), which is unsafe.
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
[1] 4775 abort      ./test
→ Desktop
→ Desktop
```

Only one input

CGI에 필요한 것은?

▼ General

Request URL: http://49.166.242.69:5000/webman/login.cgi?enable_syno_token=yes

Request Method: POST

Status Code: 200 OK

Remote Address: 49.166.242.69:5000

Referrer Policy: no-referrer-when-downgrade

Key-value input

MAgIC Fuzzer

MAgiC Fuzzer Multi-Architecture Cgi Fuzzer

CGI: IoT에 사용됨

멀티 아키텍처 지원

AFL 퍼저 기반

웹 파라미터 처리 과정

입력 값 포팅

입력 값 Wrapper

Key & Value 입력

2-ways Fuzzing

Wrapper & Seed
Generator

웹 파라미터 처리 과정

POST 방식의 입력 데이터?

Standard Input

웹 파라미터 처리 과정

GET 방식의 입력 데이터?

Standard Input 입력 불가능

웹 파라미터 처리 과정

퍼저의 입력 벡터?

Standard Input

GET 방식 파라미터 처리 과정

사용자 파라미터 입력



웹 서버: 파라미터를 환경변수에 등록



CGI: 등록된 환경변수 값을 가져와서 사용

Wrapper: Stdin to Env Var

Wrapper: Stdin to Env Var

사용자: STDIN 데이터 입력



Wrapper: 입력 값을 환경변수에 등록



Wrapper: CGI 파일 실행

Wrapper: Stdin to Env Var

```
1 #include<stdio.h>
2 #include<stdlib.h>
3
4 extern char ** environ;
5 void main(int argc, char *argv[]){
6     char s[0x100];
7     scanf("%s",s); {사용자 입력
8     setenv("BUF",s,1);
9
10    execv("./buf",NULL,environ);
11 }
```

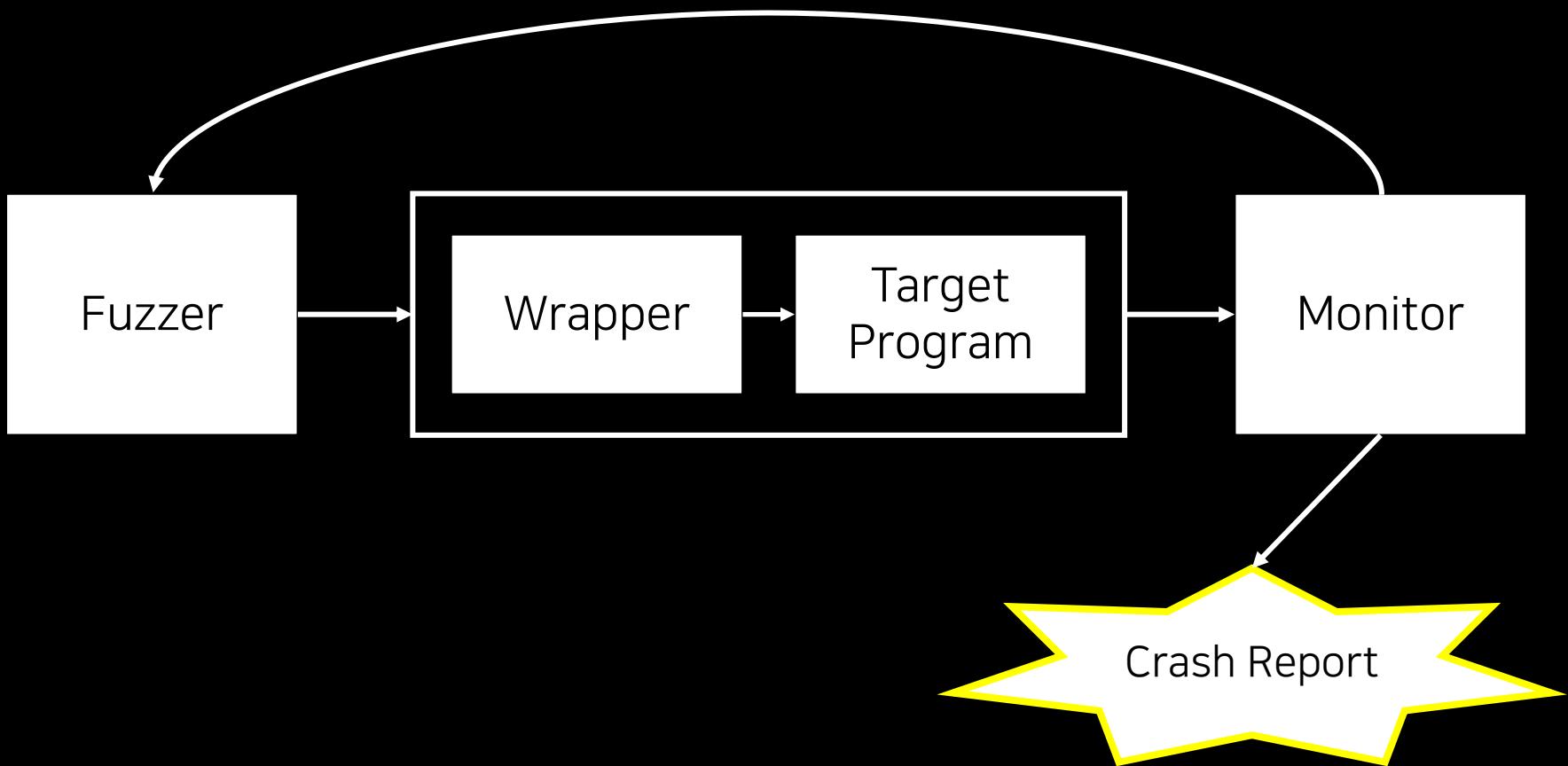
Wrapper: Stdin to Env Var

```
1 #include<stdio.h>
2 #include<stdlib.h>
3
4 extern char ** environ;
5 void main(int argc, char *argv[]){
6     char s[0x100];
7     scanf("%s",s);
8     setenv("BUF",s,1); <-- 환경변수 등록
9
10    execv("./buf",NULL,environ);
11 }
```

Wrapper: Stdin to Env Var

```
1 #include<stdio.h>
2 #include<stdlib.h>
3
4 extern char ** environ;
5 void main(int argc, char *argv[]){
6     char s[0x100];
7     scanf("%s",s);
8     setenv("BUF",s,1);
9
10    execv("./buf",NULL,environ); 실행
11 }
```

Wrapper: Stdin to Env Var



Key-value 입력

```
root@118-27-12-79:~/afl/template# ./wrapper  
qqqqqqq { Key  
qqqqqqq { Value
```

Random Input을 생성하여 퍼저를 돌려본 결과



이유?

랜덤 시드로는 유의미한 KEY 값 생성 불가능

Meaningful Key Necessary

```
1 int sub_14C60()
2 {
3     int result; // r0
4     int v1; // r0
5     int v2; // r0
6     int v3; // [sp+0h] [bp-288h]
7     char v4; // [sp+00h] [bp-288h]
8
9     cgiFormString("f_job_name", &v4);
10    result = sub_15D88(&v4);
11    if ( result == -1 )
12    {
13        v1 = cgi_escapeShellArg(&v4);
14        v2 = snprintf((char *)&v3, 0x200u, "s3 schedule delete name=%s", v1);
15        cgi_escapeShellArg_free(v2);
16        system((const char *)&v3);
17        sub_140D4(&v4);
18        xml_write_file("/etc/NAS_CFG/config.xml");
19        LIB_C_P_Config_To_MTD(1);
20        system("access_mtd \\\"cp /etc/s3.conf /usr/local/config\\\"");
21        result = cgiHeaderContentType("text/html");
22    }
23    return result;
24 }
```

유의미한 키 값

키값이 유효하지 않으면

코드 커버리지에 영향 없음

해결법?

Wrapper Generator

Wrapper Generator?

1. 유의미한 Key 값 입력 받음
2. Key 값을 소스코드에 고정
3. Wrapper 컴파일

Generated Wrapper

```
1 #include<stdio.h>
2 #include<stdlib.h>
3
4 extern char ** environ;
5 void main(int argc, char *argv[]){
6     char s[0x60000] = {};
7     char q[0x60000] = {};
8
9     sprintf(s, "cmd=%s");    키 값 고정
10    scanf("%1024s", &s);
11    strcat(s, "&meaningful_key=");
12    strcat(s, q);
13
14    setenv("QUERY_STRING", s, 1);
15    setenv("REQUEST_METHOD", "GET", 1);
16    execv("./s3.cgi", NULL, environ);
17 }
```

Key 값은 퍼저에 의해
뮤테이션 X

Meaningful Key Generation

Parsing HTML

해당 CGI 파일의
HTML 코드 파싱

Hooking

파라미터 처리 함수 후킹
인자 값 모니터링

Parsing Code

소스코드 패턴 파악하여
키 값 파싱

Strings

구현은 쉽지만
퍼징이 비효율적

Using Your Hands

힘들

Seed Issue

```
afl-fuzz 2.52b by <lcamtuf@google.com>
[+] You have 4 CPU cores and 2 runnable tasks (utilization: 50%).
[+] Try parallel jobs - see docs/parallel_fuzzing.txt.
[*] Checking CPU core loadout...
[+] Found a free CPU core, binding to #2.
[*] Checking core_pattern...
[*] Setting up output directories...
[*] Scanning 'log/_s3.cgi/cgi_s3_backup/494a7fdc/input/'...
[+] No auto-generated dictionary tokens to reuse.
[*] Creating hard links for all input files...
[*] Validating target binary...
[*] Attempting dry run with 'id:000000,orig:1.txt'...
[*] Spinning up the fork server...
[+] All right - fork server is up.
    Len = 04, map size = 26, exec speed = 4417 us
[*] Attempting dry run with 'id:000001,orig:2.txt'...

[-] Oops, the program crashed with one of the test cases provided. There are
several possible explanations:

- The test case causes known crashes under normal working conditions. If
so, please remove it. The fuzzer should be seeded with interesting
inputs - but not ones that cause an outright crash.

- The current memory limit (4.00 GB) is too low for this program, causing
it to die due to OOM when parsing valid files. To fix this, try
bumping it up with the -m setting in the command line. If in doubt,
try something along the lines of:

( ulimit -Sv $[4095 << 10]; /path/to/binary [...] <testcase >

Tip: you can use http://jwilk.net/software/recidivism to quickly
estimate the required amount of virtual memory for the binary. Also,
if you are using ASAN, see docs/notes_for_asan.txt.

- Least likely, there is a horrible bug in the fuzzer. If other options
fail, poke <lcamtuf@coredump.cx> for troubleshooting tips.

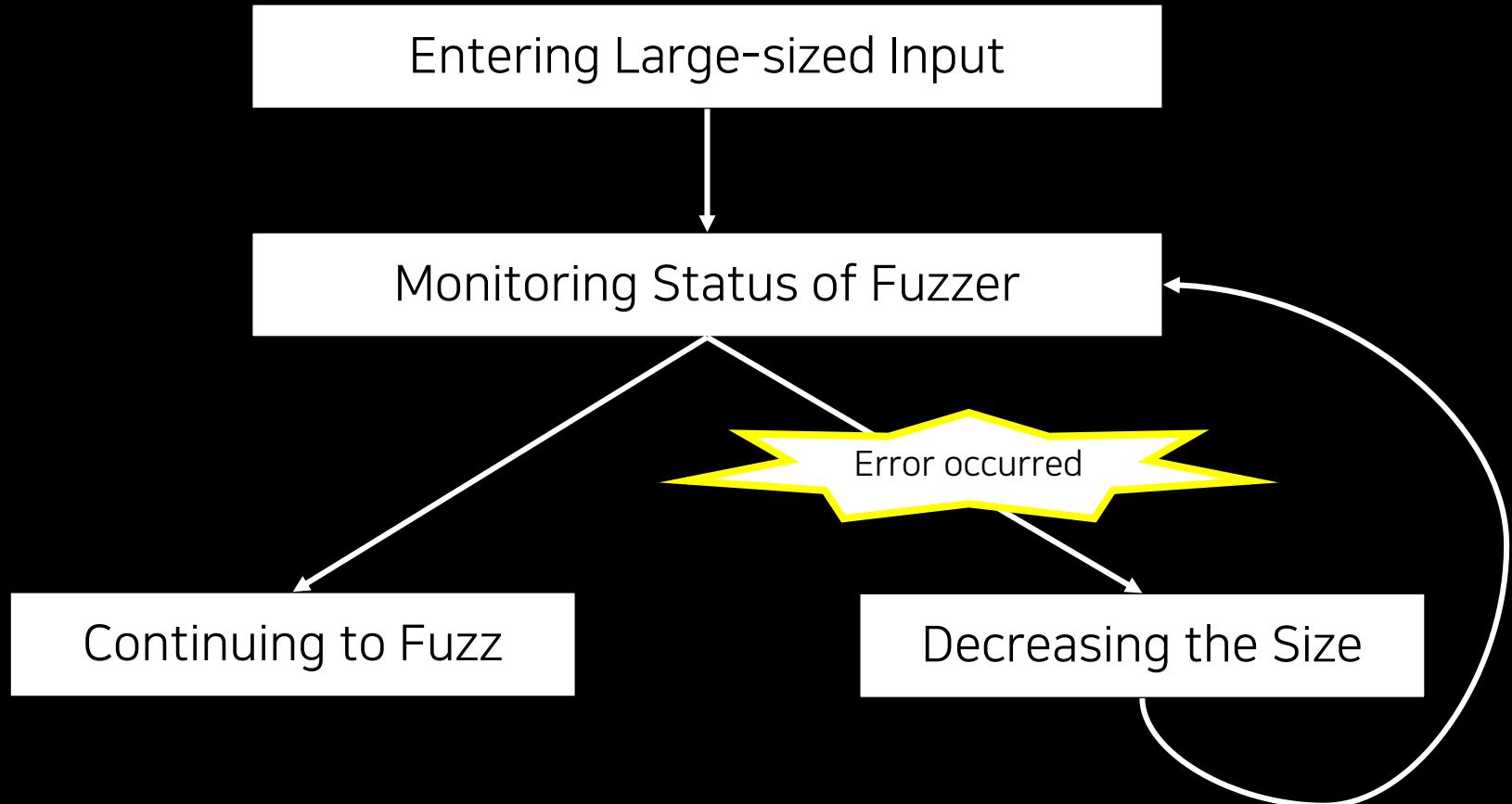
[-] PROGRAM ABORT : Test case 'id:000001,orig:2.txt' results in a crash
    Location : perform_dry_run(), afl-fuzz.c:2852
```

Initial Seed 값은
정상적인 입력 값으로
설정해주어야 함

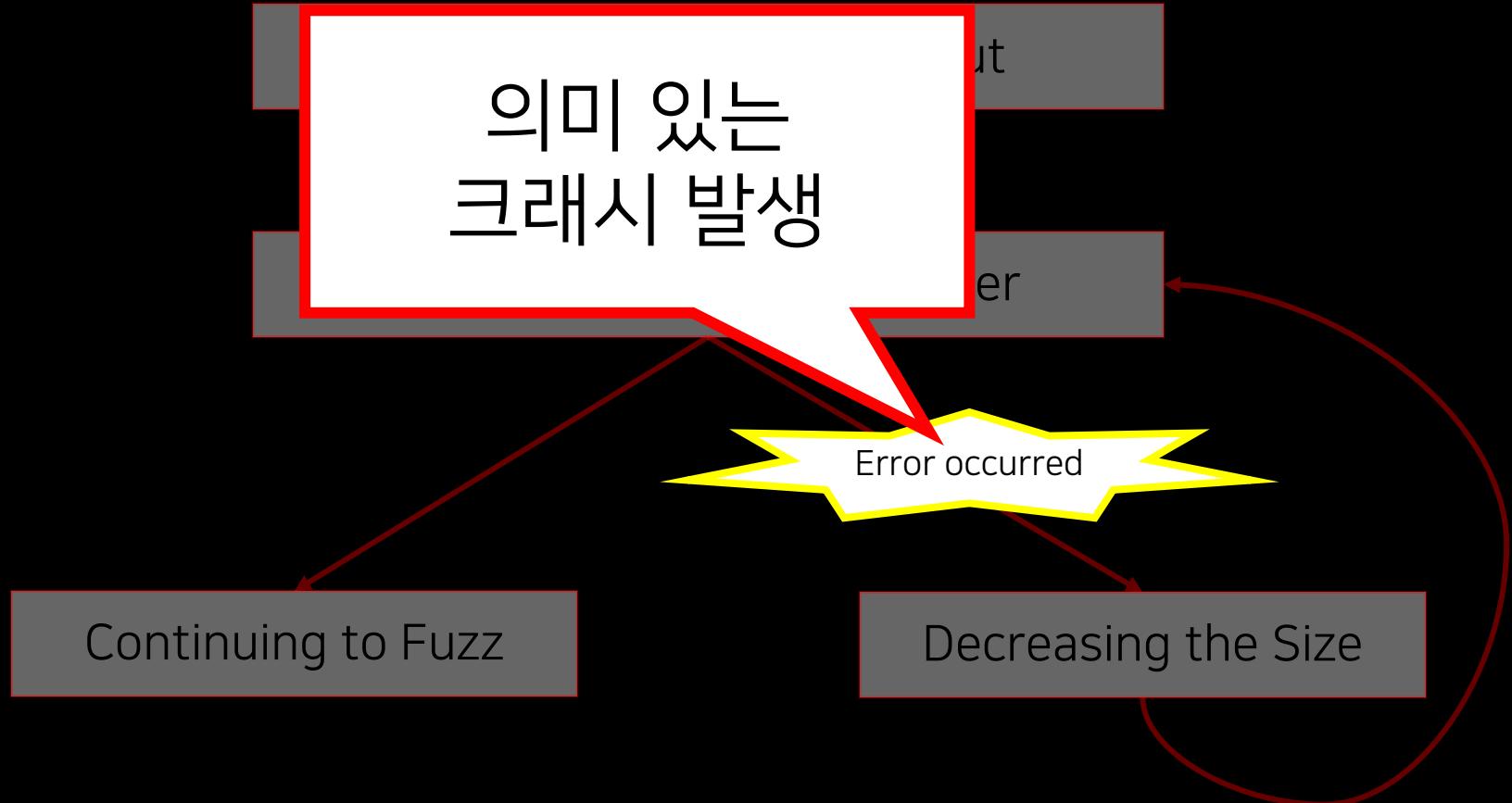
해결법?

Seed Generator

Seed Generator



Seed Generator



Lots of BOF Detected

```
cgi_s3_all_name/:
total 36
drwxr-xr-x 3 root root 4096 Nov 10 13:41 073fe6bf
drwxr-xr-x 3 root root 4096 Nov 10 13:42 1ed0eefa
drwxr-xr-x 3 root root 4096 Nov 10 13:42 50c041e5
drwxr-xr-x 3 root root 4096 Nov 10 13:42 522f7e70
drwxr-xr-x 3 root root 4096 Nov 10 13:42 5b7f61ba
drwxr-xr-x 3 root root 4096 Nov 10 13:42 ae1a0934
drwxr-xr-x 3 root root 4096 Nov 10 13:42 e7575965
drwxr-xr-x 3 root root 4096 Nov 10 13:41 e8f04441
drwxr-xr-x 3 root root 4096 Nov 10 13:42 f0891a4c

cgi_s3_backup/:
total 12
drwxr-xr-x 3 root root 4096 Nov 10 13:39 3d638397
drwxr-xr-x 3 root root 4096 Nov 10 13:39 4228f242
drwxr-xr-x 3 root root 4096 Nov 10 13:39 f4785d8c
```

Lots of BOF Detected

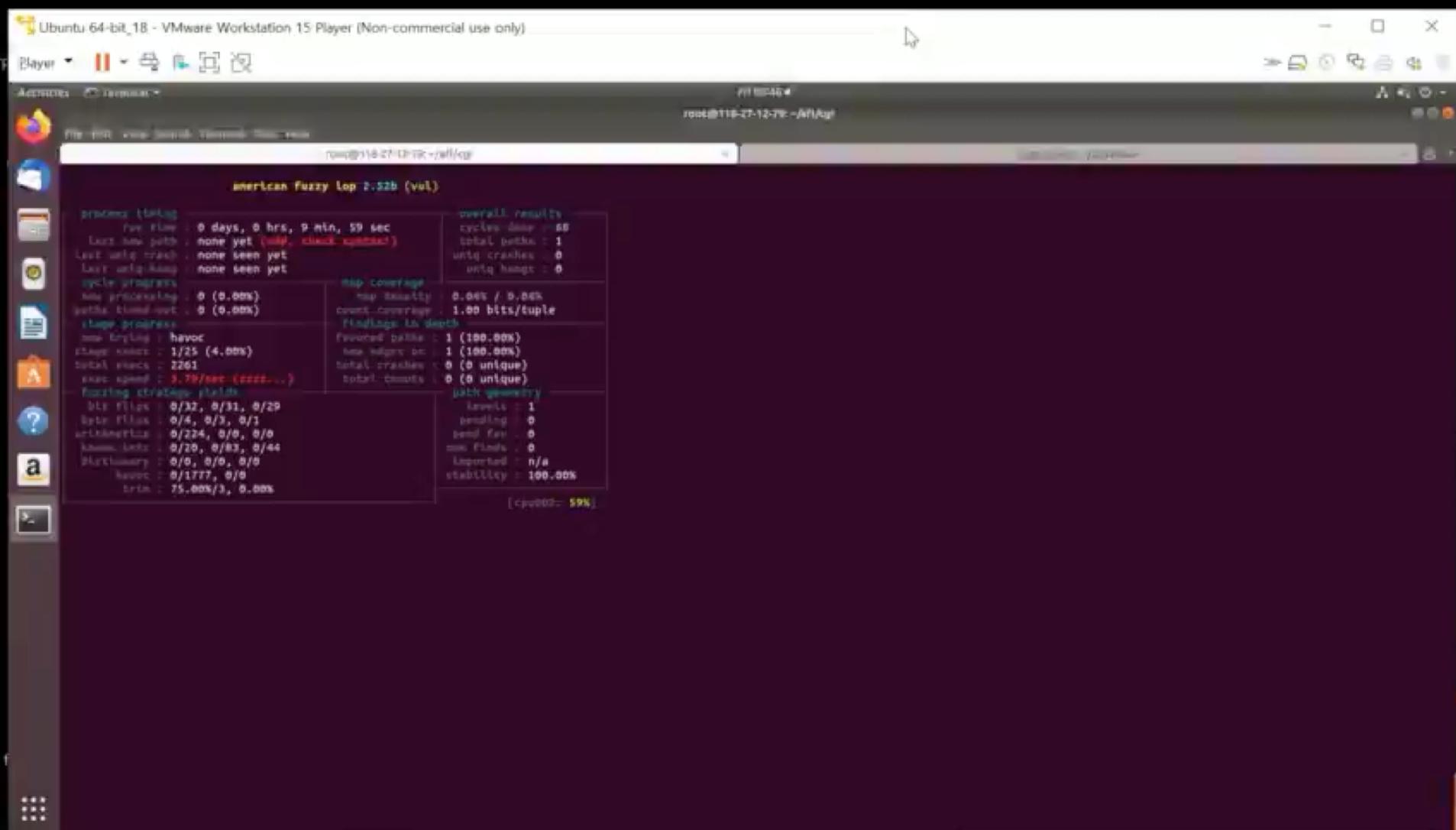
```
root@118-27-12-79:~/MAgic-Fuzzer/examples/log/_s3.cgi/cgi_s3_backup/3d638397# printf 'aaaaaaaaaaaaaaaaaaaa  
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa  
aaaaaaaa' | /root/MAgic-Fuzzer/examples/../afl-other-arch/tracers/arm/afl-qemu-trace /root/MAgic-Fuzzer  
/examples/log/_s3.cgi/cgi_s3_backup/3d638397/wrapper  
c3: can't open /etc/c3.conf  
qemu: uncaught target signal 11 (Segmentation fault) - core dumped  
Segmentation fault
```

DEMO: Seed Generator

```
root@118-27-12-79:~/MAgic-Fuzzer/examples# python wrapperGenerator.py
```

}

DEMO: MAgIC Fuzzer



Conclusion

프로젝트 성과

파일명	함수명	분류
folder_xxxx.cgi	cgi_xxxxx_xxxx_xxx	stackoverflow
xxxx_mgr	xxxxx_xxxx_xxxxx	stackoverflow
folder_xxxx.cgi	cgixxxxx_xxxxx_xxxx	stackoverflow
xxxx_mgr.cgi	cgi_xxxx	stackoverflow
xxxx_mgr.cgi	cgi_xxxx	stackoverflow
hd_xxxx.cgi	cgi_xxxx_xxxx_xxxx	stackoverflow
hd_xxxx.cgi	cgi_xxxx_xxxx_xxxx	stackoverflow
hd_xxxx.cgi	cgi_xxxx_xxxx_xxxx	stackoverflow
ve_xxxx.cgi	cgi_xxxx_xxxx_xxxx_xxxx	stackoverflow
xxxx_mgr.cgi	cgi_xxxx_xxxx	heapoverflow
xxxx_mgr.cgi	cgi_xxxx_xxxx	heapoverflow
xxxx_mgr.cgi	cgi_xxxx_xxxx	heapoverflow
xxxx.cgi	cgi_xxxx_xxxx_xxxx_xxxx	NullPointerException

프로젝트 성과

CVE-2019-18929

총 크래시 33개

CVE-2019-18930

Exploitable 취약점 10개

CVE-2019-18931

CVE 발급 중인 취약점 7개

실기기에서 유효하지 않음 16개

한국정보보호학회 논문 1편

퍼저를 하루동안만 돌려서 나온 크래시들입니다

(서버 비용이 없어요ㅠㅠ)

DEMO: Exploit WD NAS

```
~ (ssh) ~1 ~ (zsh) ~2
~ ~ ~ ~/Desktop (zsh)
applepie
ex.py
gest.py
getstest.c
hy
test.c
test.py
스크린샷 2019-07-21 오후 9.28.45.png
→ Desktop vi ex.py
→ Desktop vi test.py
→ Desktop vi poc.py
→ Desktop ls
IDA Pro (32-bit)
IDA Pro (64-bit)
a.out
applepie
ex.py
gest.py
getstest.c
hy
poc.py
test.c
test.py
스크린샷 2019-07-21 오후 9.28.45.png
→ Desktop ls -l
total 920
lrwxr-xr-x 1 delspon staff      33 5 24 17:01 IDA Pro (32-bit) -> /Applications/IDA
Pro 7.0/ida.app
lrwxr-xr-x 1 delspon staff      35 5 24 17:01 IDA Pro (64-bit) -> /Applications/IDA
Pro 7.0/ida64.app
-rwxr-xr-x 1 delspon staff    8612 7 22 14:09 a.out
drwxr-xr-x@ 13 delspon staff     416 7 7 13:21 applepie
-rw-r--r--@ 1 delspon staff    1161 7 22 20:57 ex.py
-rw-r--r--@ 1 delspon staff      87 7 22 14:11 gest.py
-rw-r--r-- 1 delspon staff     94 7 22 14:09 getstest.c
drwxr-xr-x 13 delspon staff     416 6 15 12:44 hy
-rw-r--r-- 1 delspon staff   1803 7 22 21:27 poc.py
-rw-r--r-- 1 delspon staff      72 7 20 22:04 test.c
-rw-r--r-- 1 delspon staff    332 7 21 23:06 test.py
-rw-r--r--@ 1 delspon staff  432187 7 21 21:28 스크린샷 2019-07-21 오후 9.28.45.png
→ Desktop vi ex.py
→ Desktop python ex.py
→ Desktop vi ex.py
→ Desktop python ex.py
```

Value of MAgic Fuzzer

시중에 공개된 key-value 쌍 퍼저는 존재하지 않음

멀티 아키텍처 지원으로 타겟 확장 용이

크래시 및 exploitable 취약점 탐지율 상당히 높음

몇가지 버그 픽스 및 성능 향상 후 오픈소스 공개 예정