Fuzzing

Vicente Díaz

Edge-Security www.edge-security.com
FIST Conferences www.fistconference.org

edge security

Definición

Conclusión

Creación

Ejemplo

Definición

- Es una técnica para buscar bugs en un software.
- Se basa en crear entradas semi-válidas para una aplicación.
- Las entradas deben ses:
  - Tratadas como válidas por la aplicación.
  - Suficientemente alteradas para hacer fallar a la aplicación.
- Los fallos detectados los podemos utilizar para explotar vulnerabilidades.

Usos

- Búsqueda de vulnerabilidades:
  - por parte de las propias empresas.
  - control de calidad.
  - implementaciones de protocolos.
  - investigadores de seguridad ;)

Tipos de fuzzers

- Automáticos
- Semi-automáticos
- Manuales

Definición

Conclusión

Creación

Ejemplo

Tipos de herramientas

- Standalone
- Frameworks

Ámbito de aplicación

- Protocolos (más utilizado)
- Ficheros (en auge: parsers aplicaciones)
- API´s
- Argumentos de un comando
- Entrada estándard

Funcionamiento

- Datos aleatorios
  - Encuentra muchos bugs.
  - Si el parseo es correcto, no sirve.
  - Infinito.
- Estudio previo
  - Normalmente es finito.
  - Sabemos lo que buscamos.
  - Al analizar la entrada podemos obviar bugs.
- Clasificación de resultados
  - Cuelgue de la aplicación (tiempo de respuesta).
  - Crash (debugger).
  - Reinicio.
  - Gran consulmo de memoria.

Creación de un fuzzer

- Análisis
  - longitud y tipo de los campos, inicio/fin de strings, inicio/fin datos binarios (dev/random), cadenas vacías, formato de strings, sql, carácteres de escape...
- Inconvenientes
  - Bug tras otro bug.
  - Lentitud del proceso.
  - Checksums.
  - Encriptación.
  - Compresión.

Ejemplos de cadenas

- Tamaños: negativos (-1,0x8000,0xffff1), muy grandes (0x7fff, puede provocar overflows), muy pequeños (buffer[len-2]='\0')
- Cadenas: muy largas, muchos %n, datos binarios dentro, vacías, longitud en el string, SQL injection, XSS, directory transversal, command injection
- Finales/inicios datos: '\0',NULL,']',')','}','>',...

Enfoques

- Mutación de datos:
  - modificar los datos de entrada para que sigan siendo válidos para el parser pero que causen un error.
  - método rápido y efectivo.
- Generación de datos:
  - más costoso en tiempo.
  - puede encontrar fallos que no cubre el enfoque anterior.

Definición

Conclusión

Creación

Ejemplo

Herramientas

- Algunos fuzzers:
  - Protos: varios (snmp) , java
  - Sysfuzz: syscall fuzzer, c
  - mangle*: serie de fuzzers por Michal Zalewski, c
  - pif: protocol independent fuzzer, privado

Herramientas

- Algunos frameworks:
  - Bed: pequeño framework, perl
  - Spike: muy completo, c
  - Smudge: network protocol, python
  - Peach: no sólo network, python

Ejemplo

- mangle.c

Funciona ...

- Mangle ha “petado”:
  - FreeBSD elf loading
  - openOffice
  - OpenBSD elf loading
  - osX image loading
  - macromedia flash parsing
  - Quicktime
  - mplayer
  - IE 5
  - RealPlayer
  - ....

Otro ejemplo

- http://heapoverflow.com/DFuzz.swf

Definición

Conclusión

Creación

Ejemplo

Resumen

- Probablemente, el método más usado para encontrar bugs.
- Forma rápida de buscar vulnerabilidades.
- Usar junto a un debugger para encontrar algún 0day ;)

Novedades

- BlueTooth Stack Smasher: Stress bluetooth implementations. BlueBug, BlueSnarf.
- ProtoVer LDAP TestSuite: Python, bugs en OpenLDAP, CommuniGate Pro Server, Fedora Directory Server, Lotus Domino Server, MailSite, Novell eDirectory, Sun Directory Server, ...

Herramientas comerciales

- Codenomicon
- muSecurity
- Hydra
- Spirent ThreatX

Links

- www.fistconference.org(esta presentación)
- www.phenoelit.de/stuff/Shutup.pdf
- ilja.netric.org/files/fuzzers
- events.ccc.de/congress/2005/ fahrplan/ attachments/582-paper_fuzzing.pdf
- http://www.scadasec.net/secwiki/ FuzzingTools

Más Links

- packetstormsecurity.org/UNIX/misc/scratch.rar
- antiparser.sf.net
- www.ioactive.com/v1.5/tools/index.php
- reedarvin.thearvins.com/tools.html
- felinemenace.org/ñd/SMUDGE/
- www.immunitysec.com/resources-freesoftware.shtml
- www.nologin.net/main.pl?action=codeView&codeId=54&
- www.packetfactory.net/projects/ISIC/
- ip6sic.sourceforge.net
- www.cirt.dk/tools/
- www.priestmaster.org/tools.html
- www.idefense.com/iia/labs-software.php?show=3

Gracias

- ¿Alguna pregunta?
- vdiaz@edge-security.com

edge security