Writing Secure C Code

Buffer Overruns

Dangerous Functions

http://www.informationweek.com/shared/printableArticle.jhtml?articleID=173602121 - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Back Search Favorites

Address http://www.informationweek.com/shared/printableArticle.jhtml?articleID=173602121 Go Google

InformationWeek
BUSINESS INNOVATION POWERED BY TECHNOLOGY

It Takes A Hacker To Catch One

As malicious hacking grows, the industry fights back, training future security pros to think like their adversaries

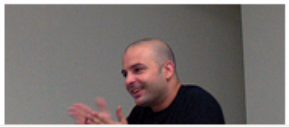
By Larry Greenemeier, InformationWeek
Nov. 14, 2005
URL: http://www.informationweek.com/story/showArticle.jhtml?articleID=173602121

Information technology professionals have been conditioned to think defensively, draping their networks with sensor-studded barbed wire and using firewalls to lock down doors and windows. Another school of thought advocates a more proactive approach to security.

New York IT consulting and job-placement firm Prime View recently held its first "Hacking-Defined Training" course, aimed at retraining laid-off IT workers in relevant and marketable skills, security being top of the list. The 10-day course goes beyond security technologies and principles, teaching students to write exploit code and hack each other's computers.

Latest Threat

Security pros and network administrators are learning the hard way that even their security vendors are having difficulty keeping up with today's malicious hackers. Cisco earlier this month issued the latest advisory for a serious Internetwork Operating System, or IOS, "heap-overflow" vulnerability that could let hackers get control of routers and switches running certain versions of the software. The heap-overflow advisory was the third security advisory Cisco issued that same week; others affected certain Cisco Airespace Wireless LAN Controllers and Cisco intrusion-prevention system devices configured by IPS Management Center version 2.1.



Prime View's weapon is Mati Aharoni, lead penetration tester with Israeli IT-security education firm See Security Technologies Ltd. Aharoni has students take a hands-on approach to learning security. "Technology itself will not stop a hacker," says Aharoni, who wears a black T-shirt with white lettering that reads, "Not Even Norton Will Protect You." "Instead," he says, "you have to use induction to

Internet

Slashdot | Second Life Hit By Massive In-Game Worm - Mozilla Firefox

File Edit View Go Bookmarks Tools Help

BBC NEWS | Technology | 'Worm' attacks Second Life world - Mozilla Firefox

File Edit View Go Bookmarks Tools Help

http://news.bbc.co.uk/2/hi/technology/6164806.stm

BBC Home News Sport Radio TV Weather Languages Search

UK version International version | About the versions Low graphics | Accessibility help

BBC NEWS

OPEN BBC News in video and audio

News services
Your news when you want it

News Front Page
Africa
Americas
Asia-Pacific
Europe
Middle East
South Asia
UK
Business
Health
Science/Nature
Technology
Entertainment

Have Your Say
In Pictures
Country Profiles
Special Reports
Programmes

RELATED BBC SITES
SPORT
WEATHER
ON THIS DAY
EDITORS' BLOG

Last Updated: Monday, 20 November 2006, 10:32 GMT

E-mail this to a friend Printable version

'Worm' attacks Second Life world

Virtual world Second Life had to close its doors for a short time on Sunday after a worm attack called grey goo.

The self-replicating worm planted spinning gold rings around the virtual world, which is inhabited by more than a million users.

Players treated the attack with a mixture of mirth and anger.

Almost every aspect of your avatar can be changed

WATCH Inside Second Life

"Can this game get any more unpredictable and exciting?" asked one user, Loretta Lurra on the official Second Life blog.

As users interacted with the rings they replicated, resulting in a slowdown on the servers used by Second Life's creators Linden Lab, in California.

Second Life has become one of the most talked about developments in cyberspace in recent years.

SEE ALSO
- Second hype or second life?
  13 Nov 06 | Technology
- Reporter's Log: A day out in Second Life
  03 Nov 06 | Technology
- The ever-expanding metaverse
  03 Nov 06 | Technology
- Online world to get news bureau
  16 Oct 06 | Technology

RELATED INTERNET LINKS
- Second Life
- Second Life blog

The BBC is not responsible for the content of external internet sites

TOP TECHNOLOGY STORIES
- Police to fingerprint on streets
- Mobiles hope to be 'smart wallet'
- Microsoft eyes Office switch test

News feeds

MOST POPULAR STORIES NOW

MOST E-MAILED | MOST READ

1 Rare zoo lion cubs poisoned
2 Blaine in giant gyroscope stunt

Sections
Main
Apple
AskSlashdot
Backslash
Books
Developers
Games
Hardware
Interviews
IT
Linux
Politics
Science
YRO

Vendors
AMD

Help

Login | Create

Search

Subscribe?

deployed a "grey goo fence" before this worm struck, but someone found a hole in it.

More Worms stories

More Games stories

String Library Routines

CS 50's library: `cs50.h`

ANSI standard string library: `string.h`

Roberts'	*ANSI*	
`GetString`	~~`strcat`~~	
`CopyString`	~~`strcpy`~~	`strdup`
	`strcmp`	`strcasecmp`
	`strstr`	

More `stdio` Functions

Std files	*Files*	*Function*
	`fopen`	open a file for read/write/append
`getc`	`fgetc`	read a single character
~~`gets`~~	`fgets`	read a string
~~`scanf`~~	`fscanf`	read formatted input
	`fread`	read multiple fixed-size elements
`putc`	`fputc`	write a single character
`puts`	`fputs`	write a string
`printf`	`fprintf`	write formatted output
	`fwrite`	write multiple fixed-size elements
	`fseek`	change the current read/write position
	`fclose`	close the file

What is Secure Code?

~~**Code without comments**~~

~~**Code that uses cryptography**~~

~~**Code that is hard to use**~~

~~**Code written in Java (or C# or …)**~~

Code designed to be robust and withstand attacks by malicious users

Realities

- **If you create an application that runs on one or more computers connected to a network, your code will be attacked.**
- **Design with security in mind from the beginning, not as an afterthought.**
- **Software contains bugs, and bugs lead to security failures.**

Buffer Overrun Attacks

Adversary's goal: program control ends up so

Com **s**

> "Buffer overflows accounted for more than 50% of all major security bugs resulting in CERT/CC advisories in 1999, and the data show that the problem is growing instead of shrinking." *Viega and McGraw, p. 135.*

Language culprit: lack of native string type and safe and easy-to-use string-handling functions in C (and C++)

Echoing the Arguments

```
int main(int argc, char *argv[])
{
    int i;
    for (i = 1; i < argc; i++) {
        printf("%s ", argv[i]);
    }
    printf("\n");
}
```

An Unsafe Version

```
void echo_arg(const char s[])
{
    char buf[MAX_BUF_SIZE];
    strcpy(buf, s);
    printf("%s ", buf);
}

int main(int argc, char *argv[])
{
    int i;
    for (i = 1; i < argc; i++) {
        echo_arg(argv[i]);
    }
    printf("\n");
}
```

An Unsafe Version (2)

```
void gotcha()
{
    printf("\nGotcha!\n");
}

void echo_arg(const char s[])
{
    char buf[MAX_BUF_SIZE];
    strcpy(buf, s);
    printf("%s ", buf);
}

int main(int argc, char *argv[])
{
    int i;
    for (i = 1; i < argc; i++) {
        echo_arg(argv[i]);
    }
    printf("\n");
}
```

Key Elements

- **Fixed-size buffer declared on stack**
- **Unsafe function writes contents of buffer**
- **Unchecked user input passed to unsafe function**
- **Adversary's input changes return address of a function on the stack**

Studying the Stack

```
printf("\nContents of stack BEFORE strcpy:\n"
     "0x%08x -- garbage\n"
     "0x%08x -- garbage\n"
     "0x%08x -- garbage\n"
     "0x%08x -- garbage\n"
     "0x%08x -- initial contents of buf\n"
     "0x%08x -- contents of EBP in main\n"
     "0x%08x -- return address\n"
     "0x%08x -- address of 1st parameter\n");
```

How to Prevent Buffer Overruns

Always validate your inputs

Never use strcpy (use strncpy)

```
#define strcpy Unsafe_strcpy
```

Fail gracefully

Rhetoric

- **Security is a process**
- **Secure the weakest link**
- **Practice defense in depth**
- **Fail securely**
- **Follow the principle of least privilege**
- **Compartmentalize**
- **Keep it simple**
- **…**

Other Similar Exploits

heap overruns

array indexing errors

Unsafe Functions (0)

```
char *strcpy(char *dst, char *src);
```

- problem: no explicit test on size of `src` string
- use `strncpy` as follows:

```
strncpy(dst, src, dst_size - 1);
dst[dst_size - 1] = '\0';
```

```
char *strcat(char *dst, char *src);
```

- problem: similar to `strcpy`

Unsafe Functions (1)

```
char *gets(char *buf);
```

- reads from stdin until linefeed or carriage return
- problem: how big should `buf` be?
- solution: use the safer

```
char *fgets(char *line,
            int maxline,
            FILE *fp);
```

Unsafe Functions (2)

```
int printf(const char *format, ...);
```

- varargs functions
- technically, format string is unnecessary

```
char *hello = "Hello world!\n");
printf(hello);
/* same as printf("%s", hello); */
```

- Danger! can use printf to write memory

```
printf("%s%n\n", hello, &num);
```

- Lesson: never let user define format string

Unsafe Functions (3)

```
char *sprintf(char *buf,
              const char *format,
              ...);
```

- very useful function, but …
- problem: how big should `buf` be?
- solution: nothing universally available
  check for `snprintf` (added in C99)

Suggested Reading

- **Books about secure coding practices**

  John Viega and Gary McGraw
  Building Secure Software
  Addison-Wesley, 2002.

  Michael Howard and David LeBlanc
  Writing Secure Code
  Microsoft Press, 2002.

- **A good read about digital security**

  Bruce Schneier
  Secrets & Lies: Digital Security in a Networked World
  John Wiley & Sons, 2000.

Websites and Mailing Lists

- **President's Strategy to Secure Cyberspace**
  - www.securecyberspace.gov
- **Computer crime and intellectual property section of the Criminal Division of the U.S. Department of Justice**
  - www.cybercrime.gov
- **BugTraq mailing lists**
  - www.securityfocus.com
  - www.ntbugtraq.com

Happy Thanksgiving!