SC3010
Computer Security

Lecture 3: Software Security (II)

Outline

- **Format String Vulnerabilities**
- **Integer Overflow Vulnerabilities**
- **Scripting Vulnerabilities**

Outline

- **Format String Vulnerabilities**
- **Integer Overflow Vulnerabilities**
- **Scripting Vulnerabilities**

printf in C

printf: print a format string to the standard output (screen).

- Format string: a string with special format specifiers (escape sequences prefixed with `%’)
- **printf** can take more than one argument. The first argument is the format string; the rest consist of values to be substituted for the format specifiers.

Examples.

- `printf(“Hello, World”);`

```
    Hello, World
```

- `printf(“Year %d”, 2014);`

```
    Year 2014
```

- `printf(“The value of pi: %f”, 3.14);`

```
    The value of pi: 3.140000
```

- `printf(“The first character in %s is %c”, “abc”, ‘a’);`

```
    The first character in abc is a
```

Format String

Format	Output	Example
d *or* i	Signed decimal integer	392
u	Unsigned decimal integer	7235
o	Unsigned octal	610
x	Unsigned hexadecimal integer	7fa
X	Unsigned hexadecimal integer (uppercase)	7FA
f	Decimal floating point, lowercase	392.65
F	Decimal floating point, uppercase	392.65
e	Scientific notation (mantissa/exponent), lowercase	3.9265e+2
E	Scientific notation (mantissa/exponent), uppercase	3.9265E+2
g	Use the shortest representation: %e or %f	392.65
G	Use the shortest representation: %E or %F	392.65
a	Hexadecimal floating point, lowercase	-0xc.90fep-2
A	Hexadecimal floating point, uppercase	-0XC.90FEP-2
c	Character	a
s	String of characters	sample
p	Pointer address	B8000000
n	Nothing printed. The corresponding argument must be a pointer to a signed int. The number of characters written so far is stored in the pointed location.	