

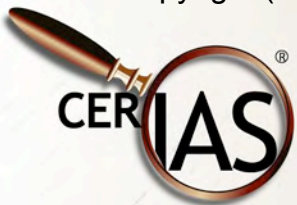
Course 2: Programming Issues, 8: Integer Overflows

Pascal Meunier, Ph.D., M.Sc., CISSP

April 4, 2006

Developed thanks to the support of Symantec Corporation,
NSF SFS Capacity Building Program (Award Number 0113725)
and the Purdue e-Enterprise Center

Copyright (2004) Purdue Research Foundation. All rights reserved.



Learning objectives

- Know the internal representation of integers
- Be able to determine when an integer overflow can occur
- Understand the consequences of integer overflows

Integers

- Fixed number of bytes
- Signed and unsigned
- Types:
 - Char
 - ❖ "char" is different from "unsigned char" and "signed char"
 - Short
 - Int
 - Long
- Extended types
 - `uint_least16_t` (integer of at least 16 bits)
 - etc...

Internal Representation

- Signed Short:
 - -1 is FFFF
 - 32767 is 7FFF
 - -32768 is 8000
- If $a = -32768$, what is $-a$?
- if $a = 32767$, what is $a+1$?

Signed Short Overflows

- $-(-32768)$ is $-32768!$
- $32767 + 1$ is 0

Internal Representation, Unsigned

- Unsigned Short:
 - 65535 is FFFF
 - 0 is 0000
- If $a = 0$, what is $a-1$?
- if $a = 65535$, what is $a+1$?

Unsigned Short Overflows

- $65535 + 1 = 0!$
- $0 - 1$ is 65535

Example Integer Overflow

```
size_t free_length; // unsigned
free_length = (sizeof(buffer1) - 1)
    - strlen(buffer1, sizeof(buffer1));
copy_length = MIN(free_length,
    strlen(first_string));
strncat(buffer1, first_string,
    copy_length);
printf("Concatenated string: '%s'\n",
    buffer1);
```

- Hint: What values can strlen return?

Silent Signed to Unsigned Conversions

- No warning, or compiler warning was ignored
- What happens when you pass a negative number to a function expecting an unsigned integer?
- `void *malloc(size_t size);`

Malloc(0) Attack Scenario

- Overflow in the size calculations can be engineered to allocate no memory
- Malloc(0) is legal, but returned value OS-dependent
 - Sun: returns pointer to the "arena"
 - Pointer to buffer of size 0, or a minimum size
- Program happily trashes the arena, or heap
 - "Fandango on core"

Questions or Comments?
