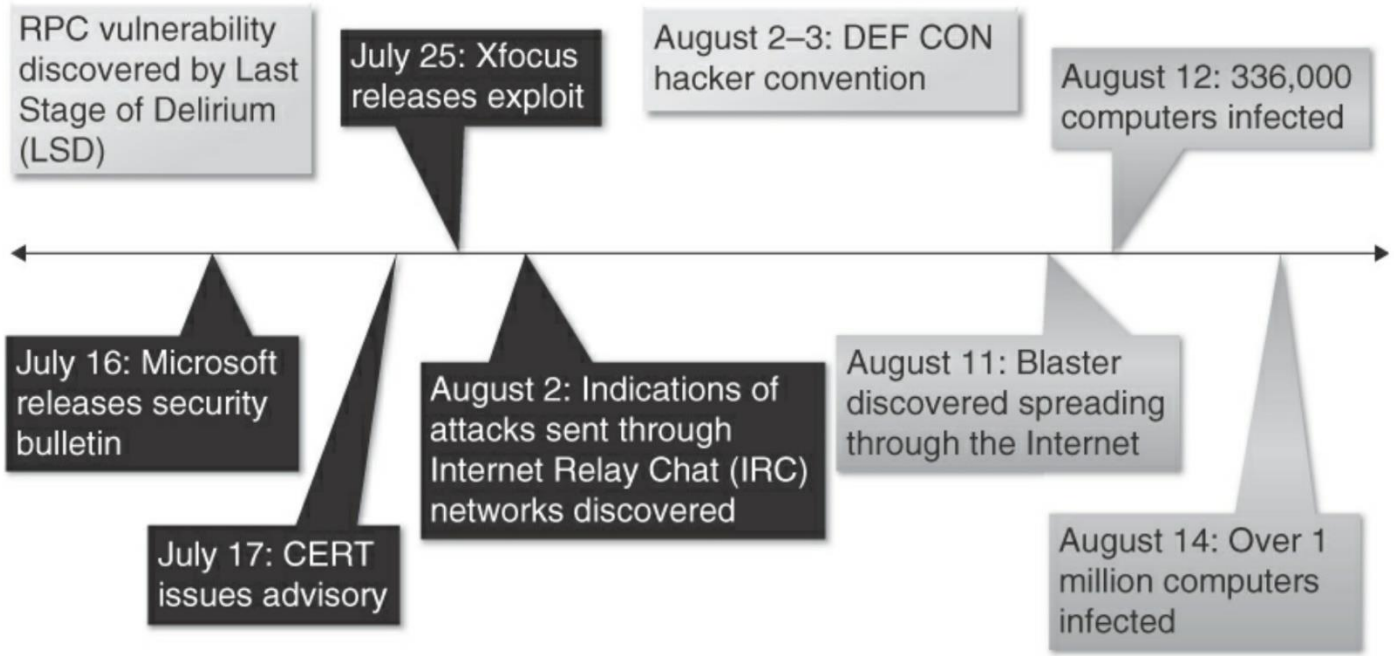
# Overview

Secure Coding in C and C++, 2nd Edition.

한양대학교 컴퓨터소프트웨어학부
임을규

# W32.Blaster.Worm

- 2003. 08. 11
- 8 million Windows systems were infected
- Buffer overflow vulnerability in RPC
- Timeline



# Vulnerable Source code



```
01    error_status_t _RemoteActivation(
02          ..., WCHAR *pwszObjectName, ... ) {
03      *phr = GetServerPath(pwszObjectName, &pwszObjectName);
04      ...
05    }
06
07    HRESULT GetServerPath(
08          WCHAR *pwszPath, WCHAR **pwszServerPath ){
09      WCHAR *pwszFinalPath = pwszPath;
10      WCHAR wszMachineName[MAX_COMPUTERNAME_LENGTH_FQDN+1];
11      hr = GetMachineName(pwszPath, wszMachineName);
12      *pwszServerPath = pwszFinalPath;
13    }
14
15    HRESULT GetMachineName(
16      WCHAR *pwszPath,
17      WCHAR wszMachineName[MAX_COMPUTERNAME_LENGTH_FQDN+1])
18    {
19      pwszServerName = wszMachineName;
20      LPWSTR pwszTemp = pwszPath + 2;
21      while ( *pwszTemp != L'\\' )
22        *pwszServerName++ = *pwszTemp++;
23        ...
24    }
```

**Figure 1.2. Flawed logic exploited by the W32.Blaster.Worm**

# Security Concepts

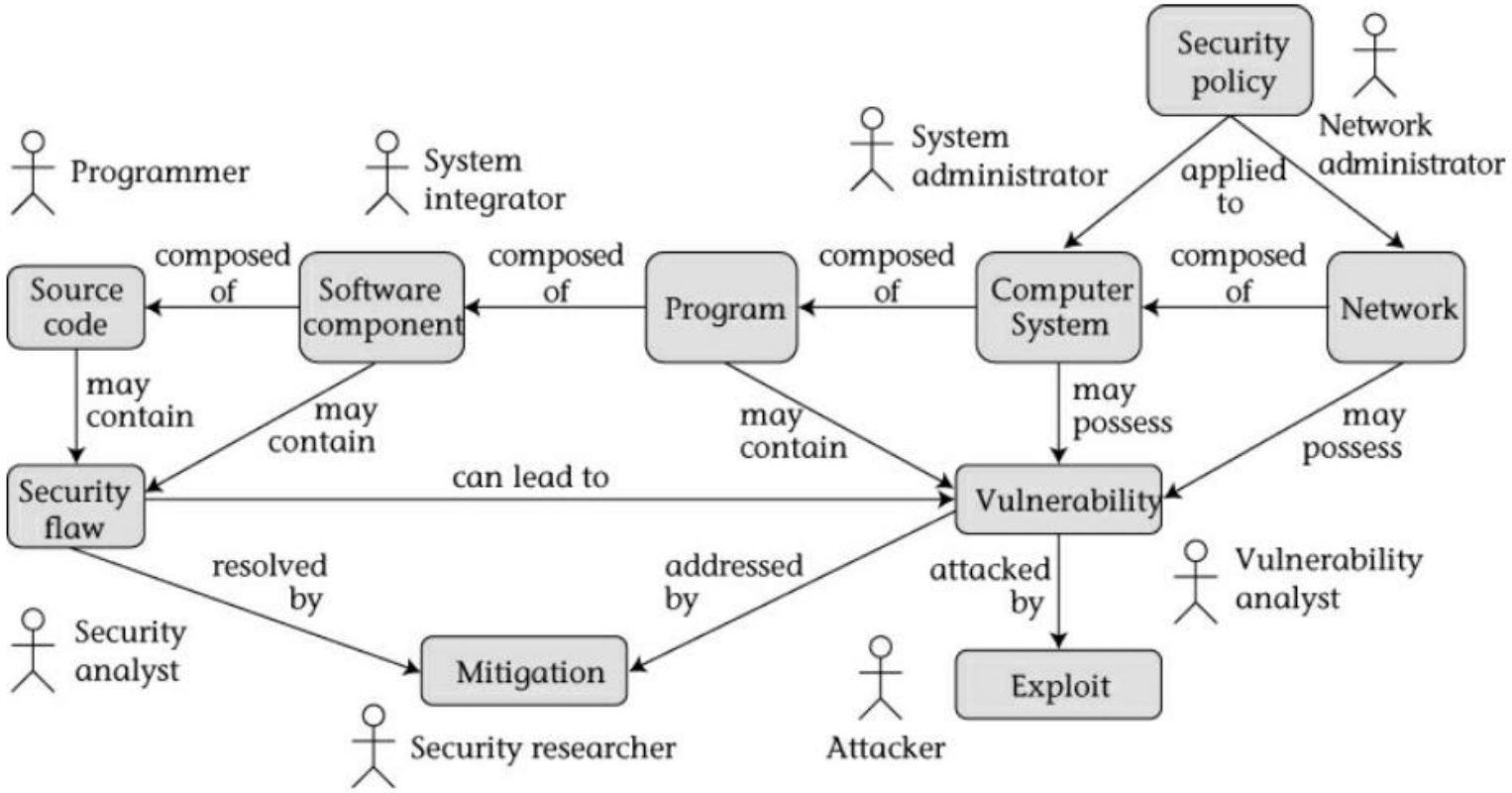



**Figure 1.4. Security concepts, actors, and relationships**

# Popular Programming Languages

| Position Jan 2013 | Position Jan 2012 | Programming Language | Ratings Jan 2013 | Delta Jan 2012 | Status |
|---|---|---|---|---|---|
| 1 | 2 | C | 17.855% | +0.89% | A |
| 2 | 1 | Java | 17.417% | -0.05% | A |
| 3 | 5 | Objective-C | 10.283% | +3.37% | A |
| 4 | 4 | C++ | 9.140% | +1.09% | A |
| 5 | 3 | C# | 6.196% | -2.57% | A |
| 6 | 6 | PHP | 5.546% | -0.16% | A |
| 7 | 7 | (Visual) Basic | 4.749% | +0.23% | A |
| 8 | 8 | Python | 4.173% | +0.96% | A |
| 9 | 9 | Perl | 2.264% | -0.50% | A |
| 10 | 10 | JavaScript | 1.976% | -0.34% | A |
| 11 | 12 | Ruby | 1.775% | +0.34% | A |
| 12 | 24 | Visual Basic .NET | 1.043% | +0.56% | A |
| 13 | 13 | Lisp | 0.953% | -0.16% | A |
| 14 | 14 | Pascal | 0.932% | +0.14% | A |
| 15 | 11 | Delphi/Object Pascal | 0.919% | -0.65% | A |
| 16 | 17 | Ada | 0.651% | +0.02% | B |
| 17 | 23 | MATLAB | 0.641% | +0.13% | B |
| 18 | 20 | Lua | 0.633% | +0.07% | B |
| 19 | 21 | Assembly | 0.629% | +0.08% | B |
| 20 | 72 | Bash | 0.613% | +0.49% | B |

**Table 1.3. TIOBE Long Term History (January 2013)**

# Brief History of C

- The C language was created the early 1970s
  - as a system implementation language for the UNIX OS
  - derived from the typeless language B (← BCPL (Basic Combined Programming Language))
- Standards
  - ANSI published a report in 1989 → ISO/IEC 9899-1990
    - C89 or C90
  - amendment: ISO/IEC 9899/AMD1:1995
    - AMD1 or C95
  - ISO/IEC 9899:1999, the second edition of the standard
    - C99
  - ISO/IEC 9899:2011
    - C11

# Descendants of C

- Concurrent C
- Objective-C
- C*
- C++ (1983)
  - C with Classes → C++
  - The Annotated C++ Reference Manual (ARM C++, 1990)
    - added exceptions and templates
  - ISO C++
    - added runtime type identification (RTTI), namespaces, std lib
    - most recent version: ISO/IEC 14882:2011 (C++11)

# C Language Standard – guiding principles

**Point 6:** Keep the spirit of C. Some of the facets of the spirit of C can be summarized in phrases like

**(a)** Trust the programmer.

**(b)** Don't prevent the programmer from doing what needs to be done.

**(c)** Keep the language small and simple.

**(d)** Provide only one way to do an operation.

**(e)** Make it fast, even if it is not guaranteed to be portable.

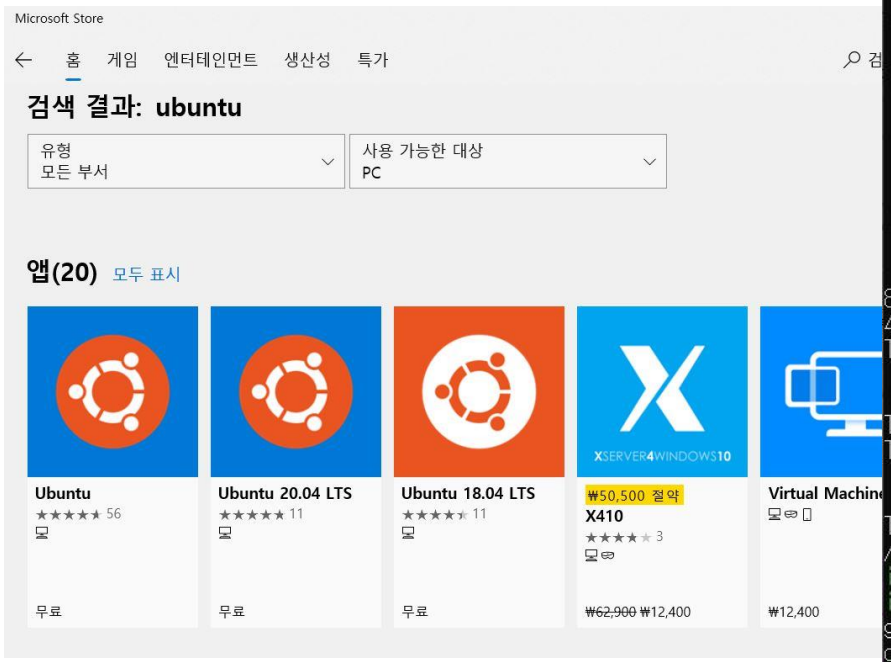
- "Undefined Behaviors"
  - Behavior can be classified as undefined because …
    - not to catch certain program errors that are difficult to diagnose
    - to avoid defining obscure corner cases that would favor one implementation strategy
    - to identify areas of possible conforming language extension

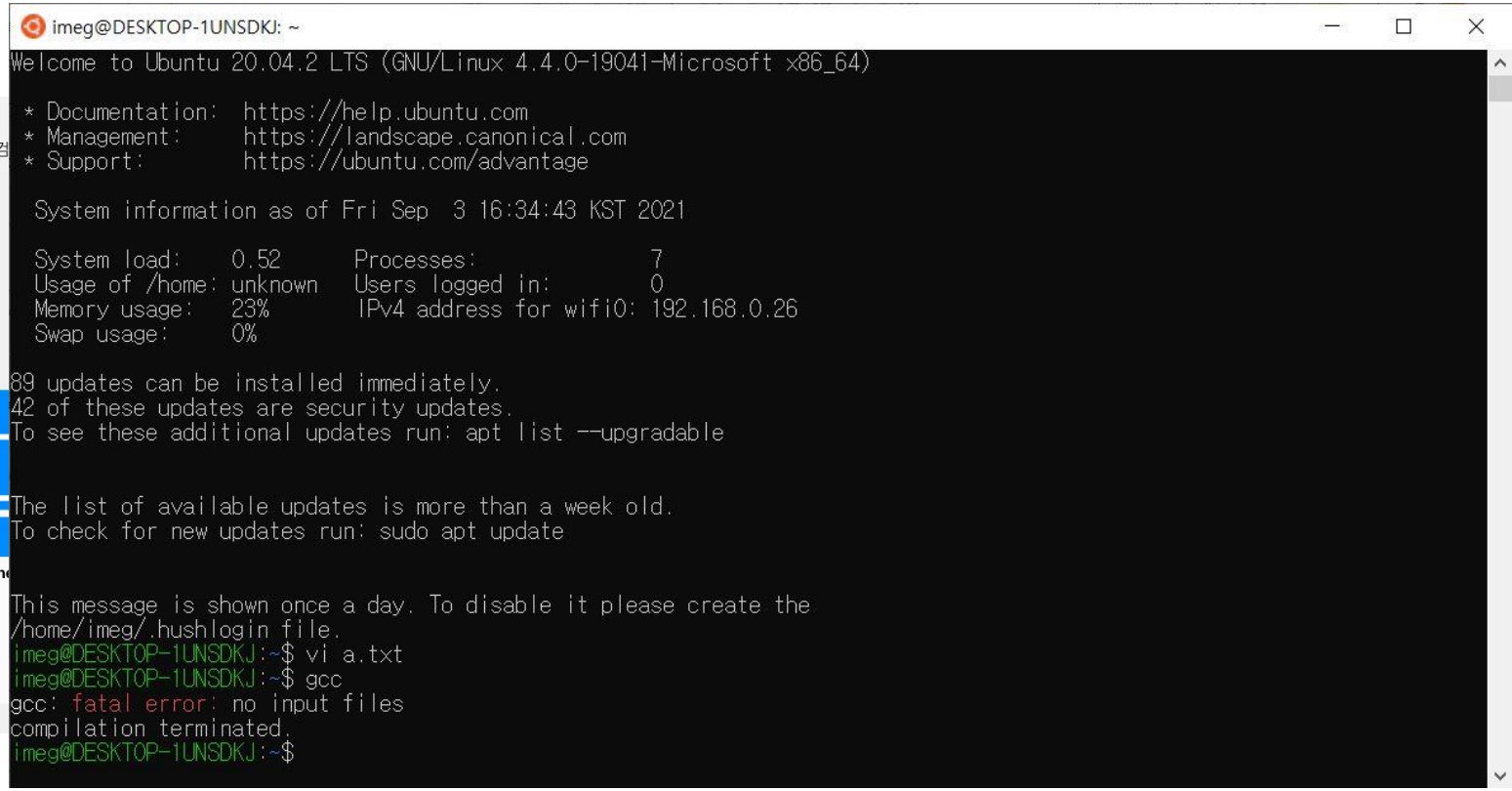
Undefined behaviors are extremely dangerous because they are not required to be diagnosed by the compiler and because any behavior can occur in the resulting program. Most of the security vulnerabilities described in this book are the result of exploiting undefined behaviors in code.

  - one of main causes of security flaws

# Windows Subsystem for Linux (WSL)

- Windows 10에서는 Linux를 설치할 수 있음.
- Microsoft Store에서 “Ubuntu” 검색
- 다운로드 후 설치




Pytanie
viechoi
질문
pregunta
vraag
Soru
dieFrage
kysymys
quesito
pergunta
percontatio
Question
&
Answer
Bonpoc
pertanyaan
fraga
savol
Kerdes
masahala
tiwen
pyetje
Intrebare
Otazka
acyynT
valasz
balasan
respuesta
vastine
답변
reactie
javob
cautraloi
resposta
dabian
odpoved
magombezi
respons
cevap
responsio
antwoord
reponse
OTBeT
xapNy
RASPUNS
replika
respond
jawaban
Antwort
svar
risposta
referat
usemaji
mabishano