

All Your Code Are Belong To Us The Principle of Most Surprise

Thank You to

@volatile_void and

@AmigaBeanbag

for the title!

SECURITY RESEARCHERS MEETUP 0x07

PATRICIA AAS

@PATI_GALLARDO



PATRICIA AAS - CONSULTANT

C++ Programmer, Application Security

Currently: TurtleSec

Previously: Vivaldi, Cisco Systems, Knowit, Opera Software Master in Computer Science - main language Java

Pronouns: she/her

@PATI_GALLARDO





UNDEFINED BEHAVIOR

"Examples of undefined behavior are memory accesses outside of array bounds, signed integer overflow, null pointer dereference, modification of the same scalar more than once in an expression without sequence points, access to an object through a pointer of a different type, etc. Compilers are not required to diagnose undefined behavior (although many simple situations are diagnosed), and the compiled program is not required to do anything meaningful."

INFINITE LOOP

```
Undefined Behavior:
int main(void) {
                                     Access out of bounds
  complex<int> delta;
  complex<int> mc[4] = \{0\};
  for(int di = 0; di < 4; di++, delta = mc[di]
    cout << di << endl;</pre>
```

INFINITE LOOP

Want to give it a try?

Compiler Explorer

https://godbolt.org/g/TDjM8h

Wandbox

https://wandbox.org/permlink/aAFP2bMjA3um3L4K

Github



SCHRÖDINGER'S VARIABLE

```
int main(void)
{
bool b:
if (b)
  printf("true\n");
if (!b)
  printf("false\n");
}
```

Undefined Behavior: Access to uninitialized variable

```
gcc 4.7.1 -00

true
false
```

SCHRÖDINGER'S VARIABLE

Want to give it a try?

```
Compiler Explorer (Gcc 4.7.1 -00)
```

```
https://godbolt.org/z/YnIDYj
```

Compiler Explorer (Clang 7.0.0 -03)

https://godbolt.org/z/00v5WP



- <u>Don't reason</u> about undefined behaviour
- Assume that it crashes or is never executed
- Changing compiler, compiler
 version or optimization level
 can break your application





CWE-14: COMPILER REMOVAL OF CODE TO CLEAR BUFFERS

```
void GetData(char *MFAddr) {
    char pwd[64];
    if (GetPasswordFromUser(pwd, sizeof(pwd))) {
        if (ConnectToMainframe(MFAddr, pwd)) {
            // Interaction with mainframe
        }
    }
    memset(pwd, 0, sizeof(pwd));
}
Dead store: removed by
    the optimizer
}
```

SEI: MSCO6-C. BEWARE OF COMPILER OPTIMIZATIONS

SEI: MEMO3-C. CLEAR SENSITIVE INFORMATION STORED IN REUSABLE RESOURCES

CWE-14: COMPILER REMOVAL OF CODE TO CLEAR BUFFERS

Want to give it a try?

https://godbolt.org/g/FpEsht

SEI: MSCO6-C. BEWARE OF COMPILER OPTIMIZATIONS

SEI: MEMO3-C. CLEAR SENSITIVE INFORMATION STORED IN REUSABLE RESOURCES

MEMSET_S: ZEROING MEMORY

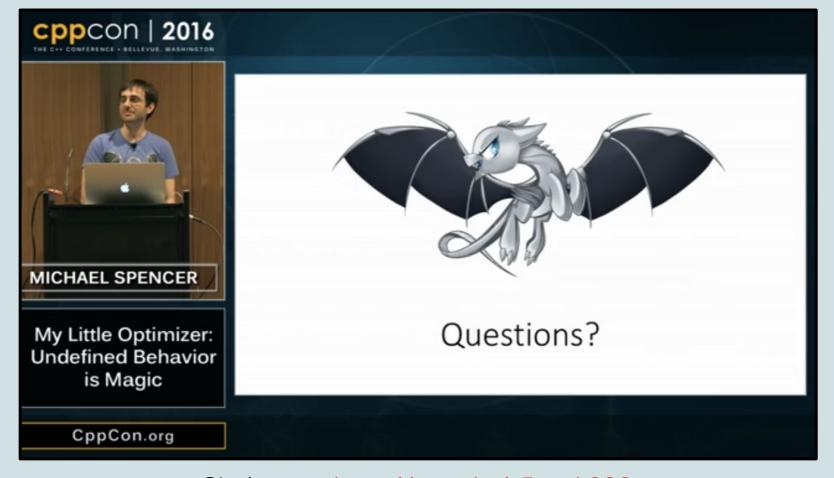
@PATI_GALLARDO

```
// Compliant Solution (C11)
memset_s(pwd, 0, sizeof(pwd));

// Windows Solution
SecureZeroMemory(pwd, sizeof(pwd));
```

SEI: MSC06-C. BEWARE OF COMPILER OPTIMIZATIONS

SEI: MEMO3-C. CLEAR SENSITIVE INFORMATION STORED IN REUSABLE RESOURCES



@Bigcheesegs https://youtu.be/g7entxb00Cc

Photos from pixabay.com

Patricia Aas, **TurtleSec**@pati_gallardo



