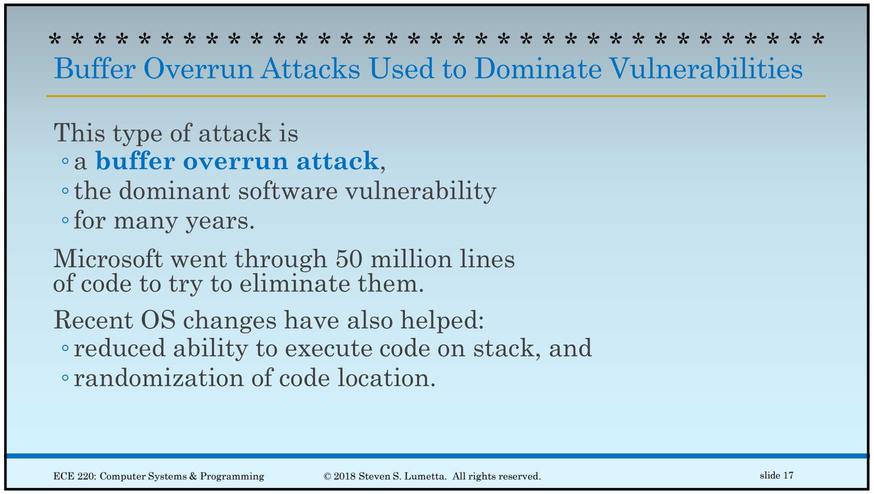


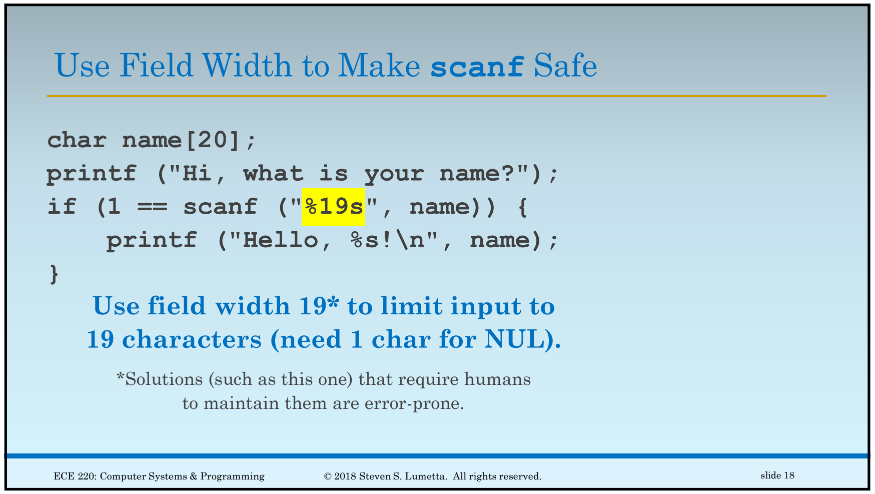
* *

Buffer Overrun Attacks Used to Dominate Vulnerabilities

This type of attack is
- a **buffer overrun attack**,
- the dominant software vulnerability
- for many years.

Microsoft went through 50 million lines of code to try to eliminate them.

Recent OS changes have also helped:
- reduced ability to execute code on stack, and
- randomization of code location.

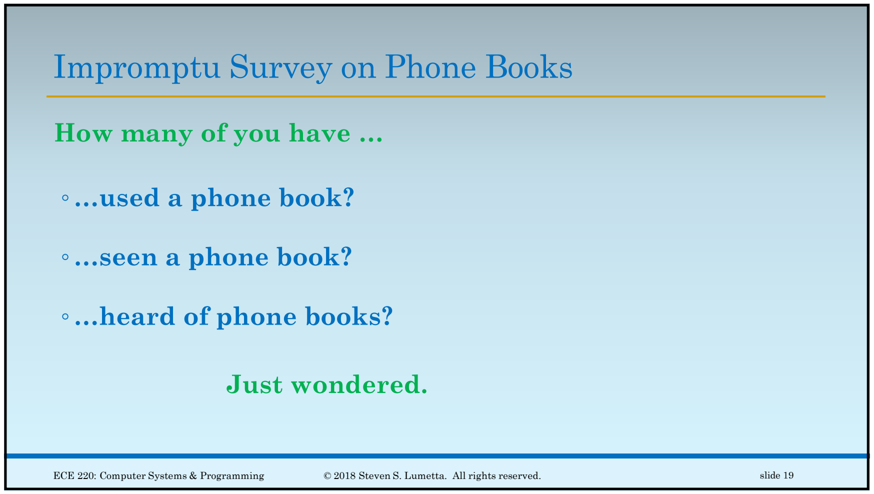


Use Field Width to Make **scanf** Safe

```
char name[20];
printf ("Hi, what is your name?");
if (1 == scanf ("%19s", name)) {
    printf ("Hello, %s!\n", name);
}
```

Use field width 19* to limit input to 19 characters (need 1 char for NUL).

*Solutions (such as this one) that require humans to maintain them are error-prone.

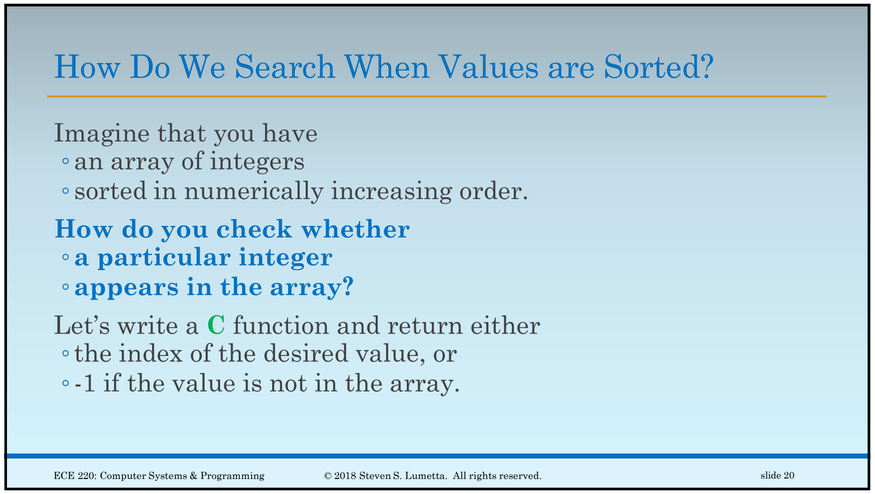


Impromptu Survey on Phone Books

How many of you have …

- **…used a phone book?**
- **…seen a phone book?**
- **…heard of phone books?**

Just wondered.



How Do We Search When Values are Sorted?

Imagine that you have
- an array of integers
- sorted in numerically increasing order.

How do you check whether
- **a particular integer**
- **appears in the array?**

Let's write a **C** function and return either
- the index of the desired value, or
- -1 if the value is not in the array.