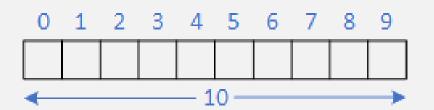# ARRAYS AND SECURITY

C++ does not automatically check array indexes

Delroy A. Brinkerhoff

- A "buffer" is an array

- Indexing an array out-of-bounds is also known as:
  - Buffer overflow
  - Buffer overrun

- Trying to put more data into the array or buffer than it can hold

- Like trying to overfill a glass

- Challenging errors to find

0	1	2	3	4	5	6	7	8	9

←——————— 10 ———————→

INDEXING AN ARRAY OUT-OF-BOUNDS

VALIDATE USER INPUT

```
Glass  glasses[3];
        . . . .
cin >> destination;
cout << "Pour TO glass:   <1, 2, or 3>: ";
cin >> source;
cout << "Pour FROM glass: <1, 2, or 3>: ";

        . . . .
if (source > 0 && source <= 3 && destination > 0 && destination <= 3)
    glasses[destination - 1].pour(glasses[source - 1]);
else
    cerr << "Glasses must be numbered 1, 2, or 3" << endl;
```

GUARD INDETERMINATE LOOPS

```cpp
int        scores[100];
int        score;
int        count = 0;

cout << "Enter a score (-1 to stop): ";

cin >> score;
while (score != -1 && count < 100)
{
        scores[count++] = score;
        cin >> score;
}
```

```cpp
int        scores[100];
int        count = 0;

cout << "Enter a score (-1 to stop): ";

do
{
        cin >> scores[count++];
}while (scores[count - 1] != -1 && count < 100);
count--;                // discard the -1
```

VALIDATE INDEX CALCULATIONS

```
for (…i …)
        for (…j …)
                …array[i - j] …
```

PASS ARRAYS AS TWO ARGUMENTS

```
const int size = 8;
int scores[size];
        . . .
void function(scores, size);
```