



Memory Corruption

Buffer Overflows for Beginners



Buffer overflows are...

ancient

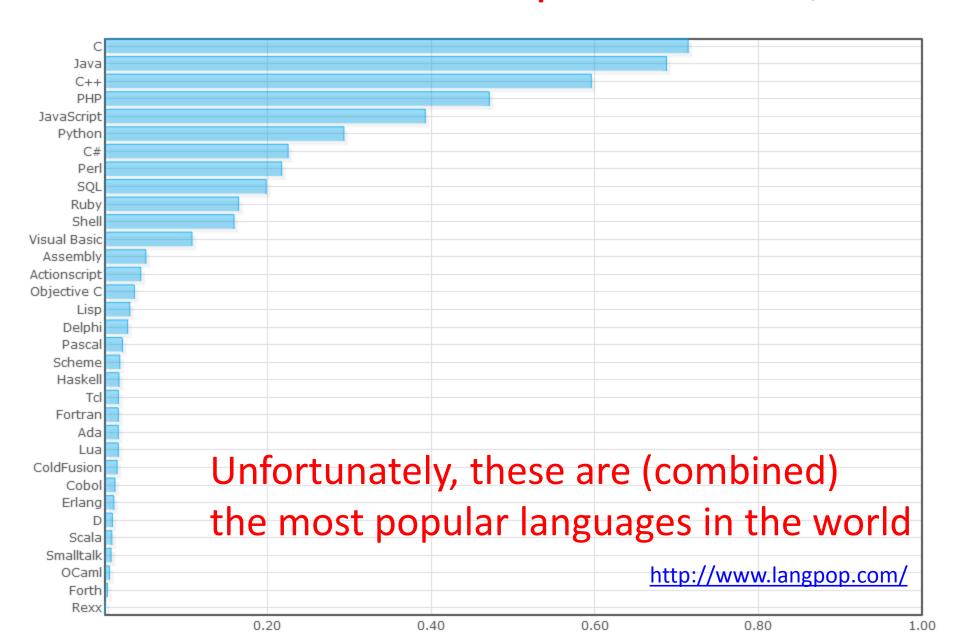
- First discussed in a US Air Force document in 70s
- Used in the first Internet Worm (<u>the Morris Worm</u>)
- Still perannually in SANS' Top 3 Most Dangerous
 Programming Errors
- One of the most important weapons in the hands of the attacker

simple

- The basic idea can be grasped by everyone
- Very advanced versions are also possible



Buffer overflows are a problem in C/C++



Roadmap

- First: general idea
 - How does a computer work?
 - Function calls, stack, etc.
 - Stylized buffer overflow
 - → Toy processor
- Next: for real
 - real code and real CPU
 - Real buffer overflows
- Then: counter measures
 - Canaries
 - DEP
 - ASLR





Roadmap

- First: general idea
 - How does a computer work?
 - Function calls, stack, etc.
 - Stylized buffer overflow
 - → Toy processor
- Next: for real
 - real code and real CPU
 - Real buffer overflows
- Finally: counter-measures
 - Canaries
 - DEP
 - ASLR



