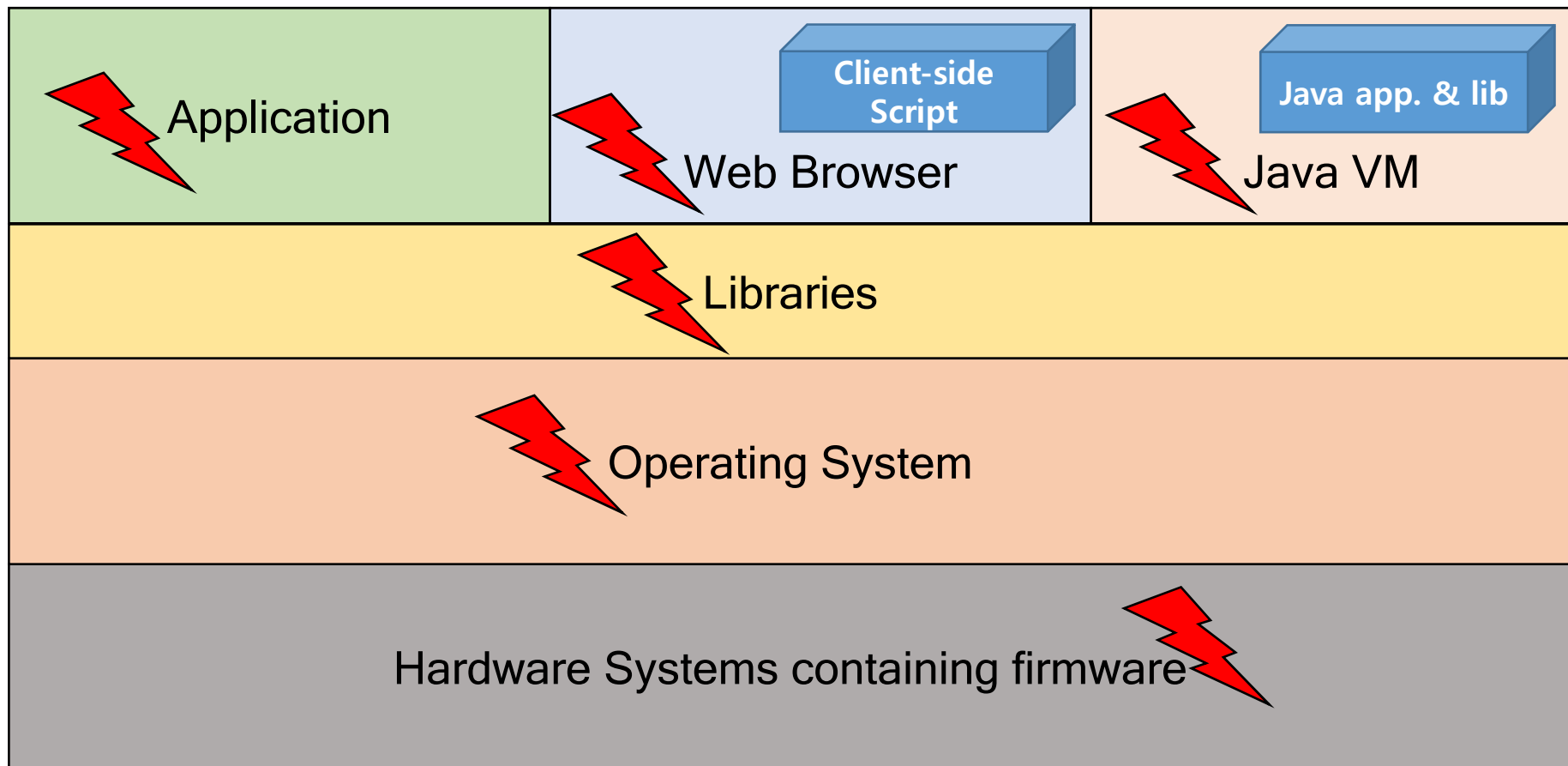2018/07/07 @ CodeEngn 15

Memory attacks and defenses

Jong-Hyouk Lee (jonghyouk@smu.ac.kr)

Protocol Engineering Lab., Sangmyung University
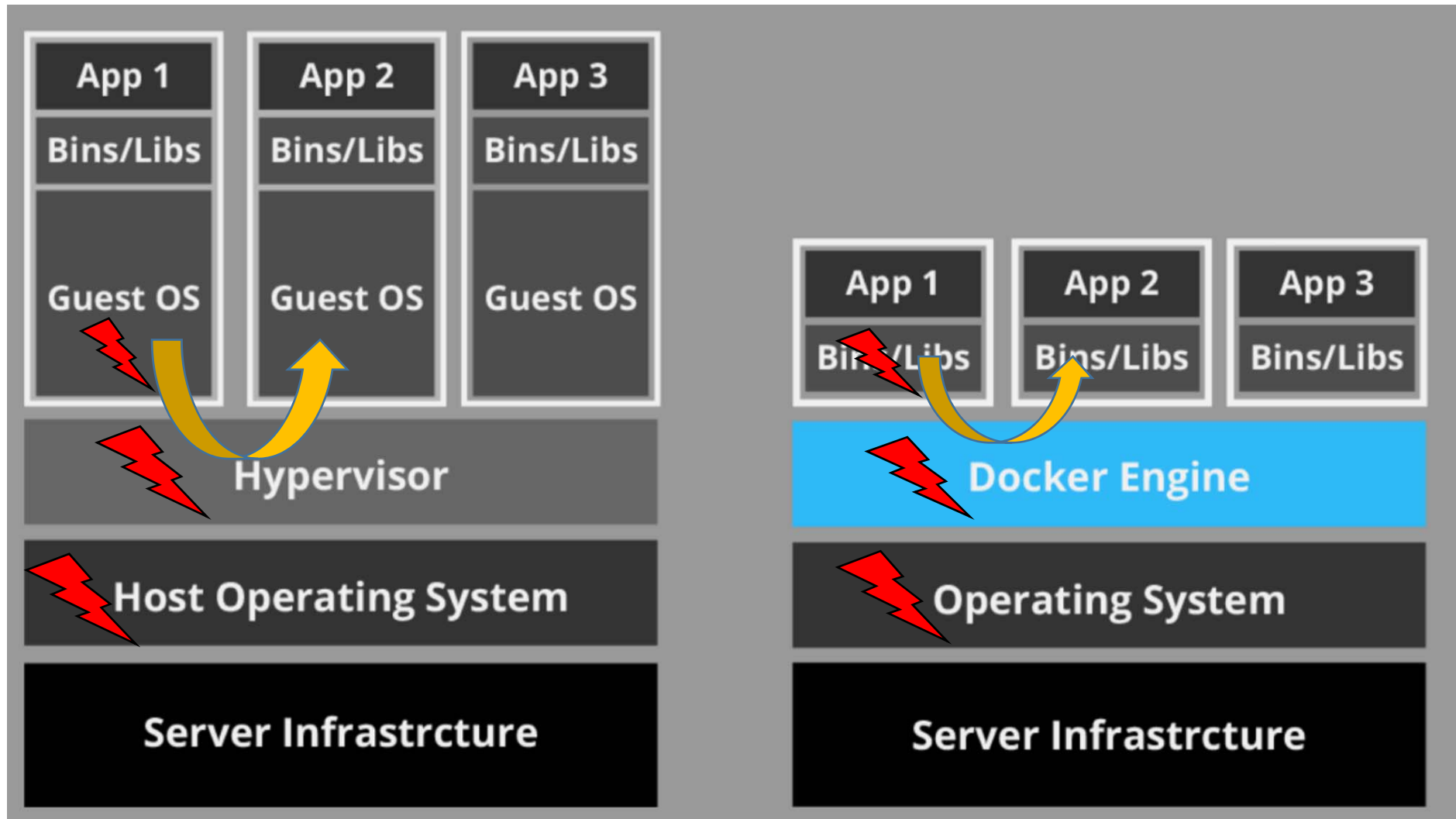
Still memory errors are problems?

- Unsafe languages like C/C++ are still very popular
  - Those will be replaced by others soon?

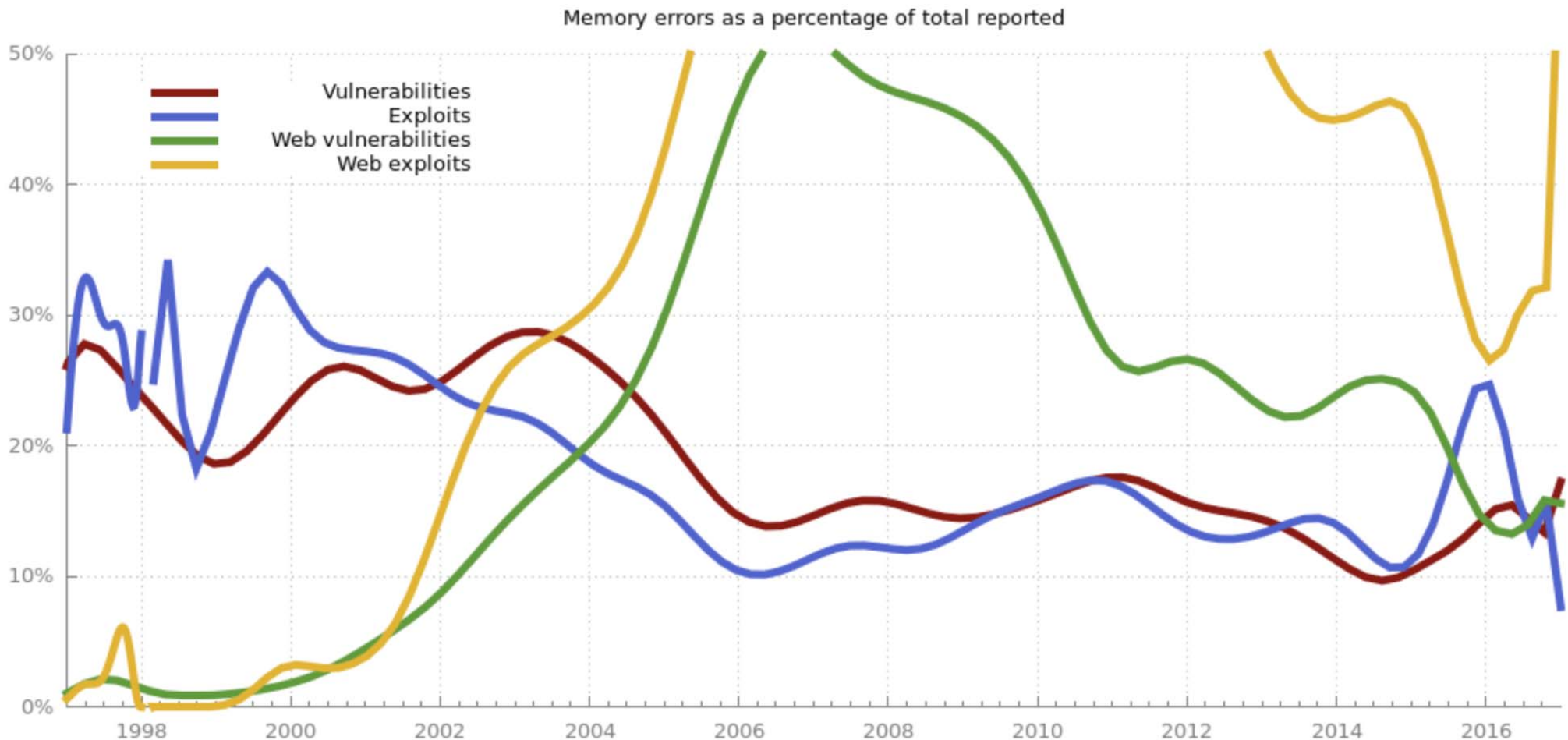|		
⚡ Application	⚡ Client-side Script Web Browser	⚡ Java app. & lib Java VM
⚡ Libraries		
⚡ Operating System		
Hardware Systems containing firmware ⚡		

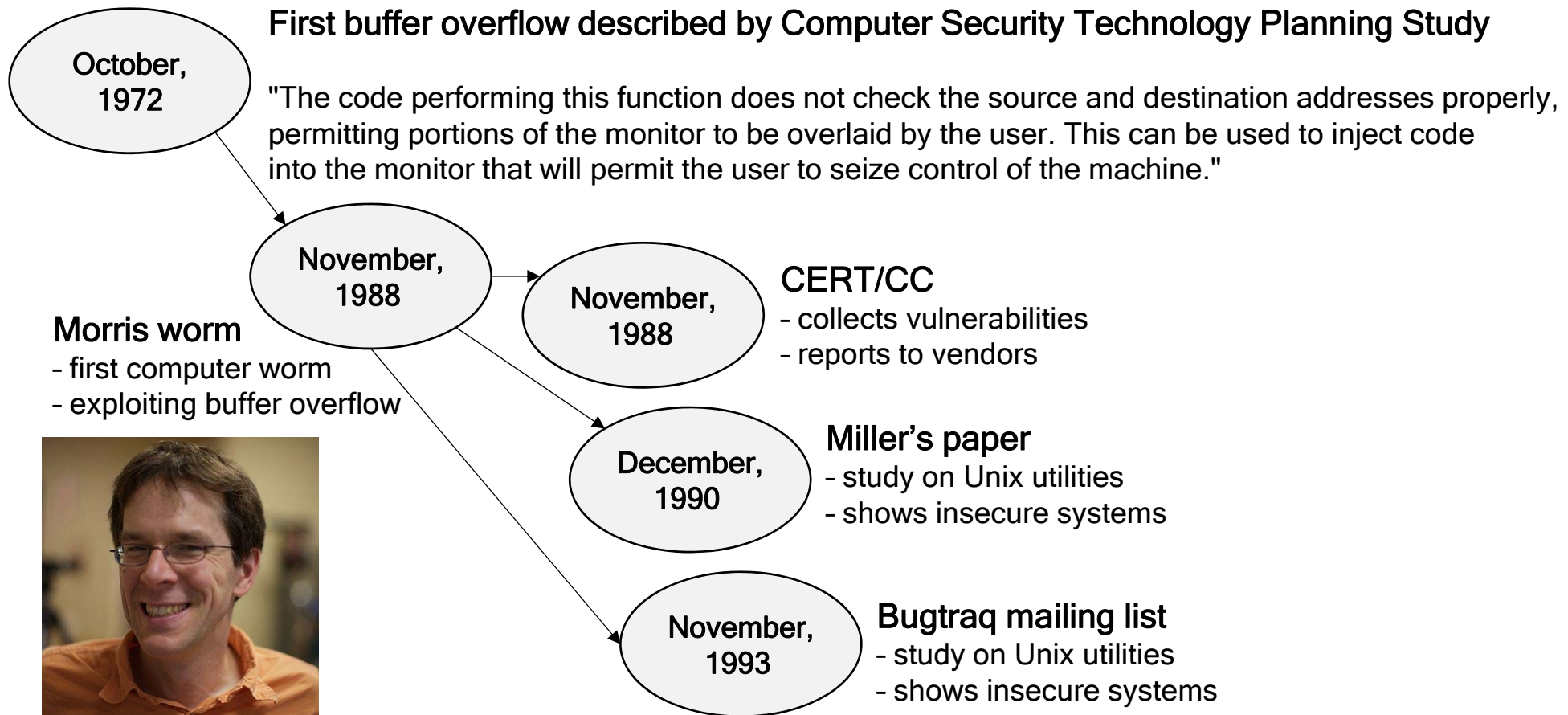# Still memory errors are problems?

- System level breaking in cloud computing

Still memory errors are problems?

- Statistics show …

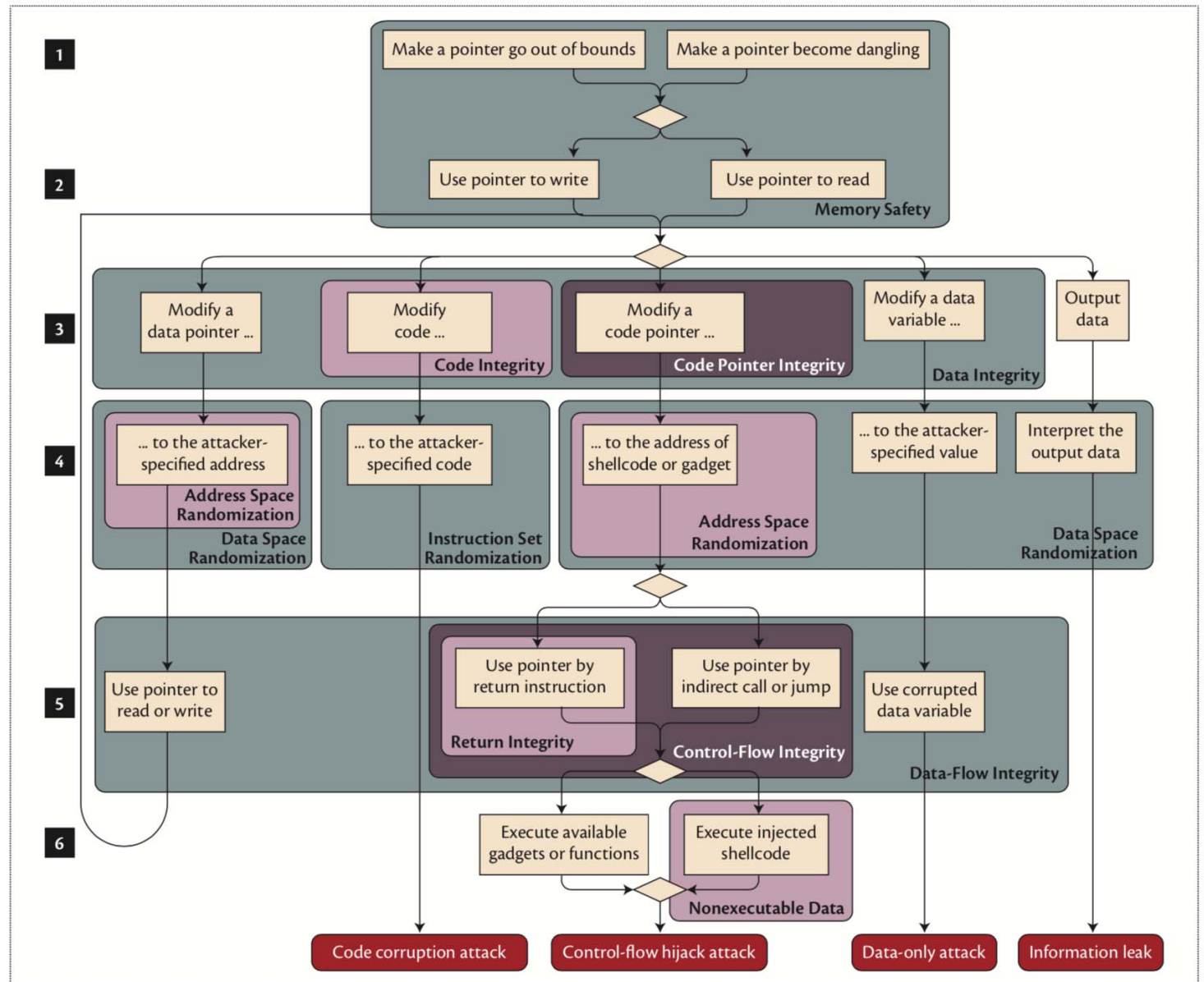Percentage of memory error vulnerabilities and exploits (including web)

Memory errors as a percentage of total reported

Some history?

First buffer overflow described by Computer Security Technology Planning Study

"The code performing this function does not check the source and destination addresses properly, permitting portions of the monitor to be overlaid by the user. This can be used to inject code into the monitor that will permit the user to seize control of the machine."

October, 1972

November, 1988

November, 1988

CERT/CC
- collects vulnerabilities
- reports to vendors

Morris worm
- first computer worm
- exploiting buffer overflow

December, 1990

Miller's paper
- study on Unix utilities
- shows insecure systems

November, 1993

Bugtraq mailing list
- study on Unix utilities
- shows insecure systems

Thanks!

이종혁 (jonghyouk@smu.ac.kr)