Improving Software Security and Reliability
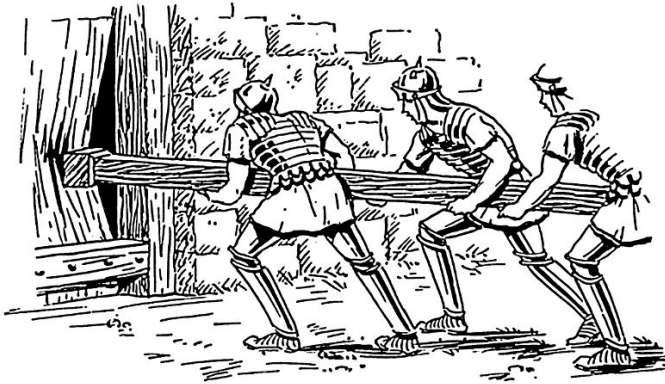
Georgios Portokalidis, Department of Computer Science

Attack and Harden Harden Software
ONR, Collab. with Columbia U
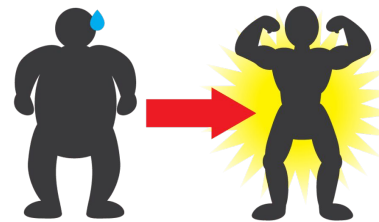
Test defenses through offense

Harden software by strengthening and developing new defenses

Adaptive Binary Debloating and Security
ONR, Collab. with Columbia and Brown U

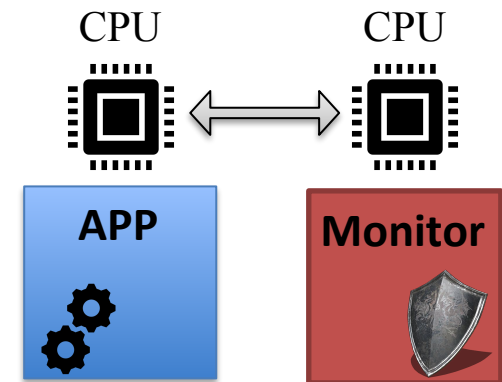Software bloat degrades performance and security

Disable **unused** and **unwanted** software components using binary analysis
- **Restrict** application capabilities to what they need
- **Adapt** over time
- **Harden** remaining components

HW-assisted Software Monitoring
DARPA

Offload security monitoring on spare core

Efficiently communicate application run-time information to monitor