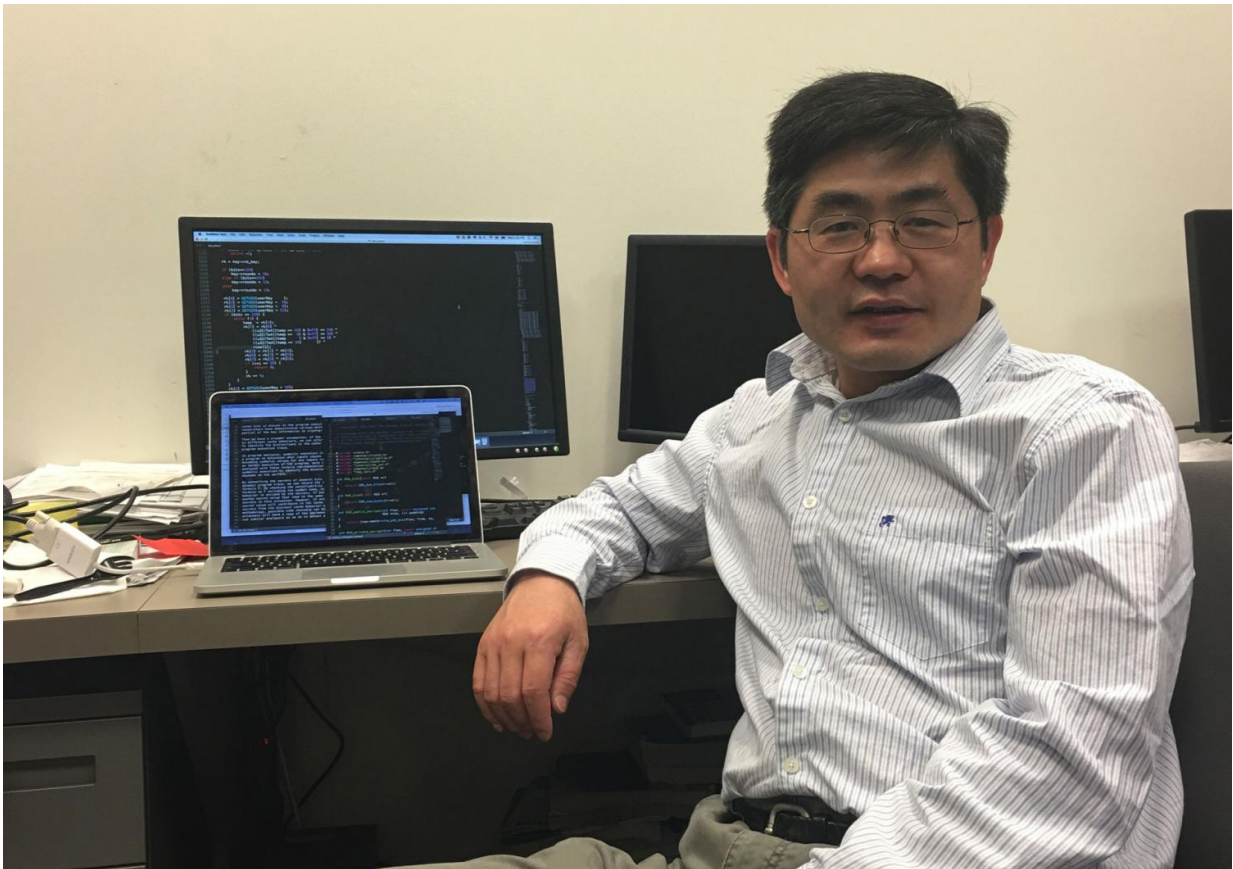


Shedding the fat: ONR explores ways to trim software bloat, improve security

July 12 2016



Dr. Dinghao Wu in his lab at Penn State University. Wu is one of several researchers sponsored by the Office of Naval Research to reduce software bloat, a condition where updated software runs slower because of repetitive code, requiring more memory -- and becoming more vulnerable to cyber attacks. Credit: Photo courtesy of Dr. Dinghao Wu

Have you ever upgraded your software program or app, only to find it didn't seem to perform as well as the older version? The problem most likely was caused by software bloat, a condition where updated software runs slower because of repetitive code, requiring more memory—and becoming more vulnerable to cyber attacks.

"Software bloat isn't only a nuisance or inconvenience," said Dr. Sukarno Mertoguno, a program officer in the Office of Naval Research's (ONR) C4ISR Department. "It also presents a serious security risk, since the additional [code](#) could offer hackers more entry points into a [software program](#)."

Security is especially important given ONR's current efforts to design the Naval Tactical Cloud—a multiyear initiative to harness the power of cloud computing and bring big data capabilities to the warfighting environment.

To ensure the Navy's cloud and other computing efforts run more securely and efficiently, ONR is supporting the work of researchers like Dr. Dinghao Wu at Pennsylvania State University and Dr. Harry Xu at the University of California, Irvine.

Software bloat is a big problem today because of how code is written and compiled. Past generations of coders wrote new, individualized code for each program upgrade, adding only what was needed to improve performance.

Thanks to voracious consumer appetites for [software](#) features and faster product rollouts, modern coders use pre-made libraries to meet demand. The problem is these libraries contain both the new code and the repetitive code from previous software versions. Downloading the libraries actually installs both sets of code in an upgrade—creating layers of redundant, unused and outdated functions that slow down computer

running time.

Then there's the security issue. "A bloated software system contains a larger code base that could lead to more vulnerabilities and greater entry platforms for hackers and cyber terrorists," said Wu. "After gaining access to a system, a hacker can use the code—even unused, older code—for malicious purposes."

Using Java, among the world's most widely used computer programming languages, Wu and his team at Penn State created a tool called [JRed](#), which can read thousands of lines of code in seconds. Through a complex algorithm, JRed applies predefined rules to the code of software upgrades and then identifies and removes bloated, repetitive code. JRed has demonstrated it can shrink software bloat by approximately 50 percent, resulting in faster running times.

Xu and his group at UC Irvine also used Java in their research. However, they designed an optimization technique called Library Auto-Selection, or LAS.

LAS creates "shadow libraries" that can update existing software by pinpointing areas of bloat and adding only the necessary code and data needed for upgrade—skipping the repetitive code. The shadow library then is disabled through an automatic switch mechanism, eliminating the risk of repetition or cyber attack. Xu said his LAS method has trimmed software bloat significantly and improved run time speed by more than 70 percent.

"Aside from concerns about effectiveness and cost savings, reducing software bloat is critical to the capabilities of the Navy and Marine Corps," said Xu. "Military-focused software plays such a large role in the warfighting environment—from carrying out mission-critical tasks to managing confidential data—and must be even more resistant to cyber

attacks than software available to the public."

The next step in Wu's and Xu's research involves cutting software bloat in mobile applications and large-scale cloud-computing networks. Their work is part of ONR's [Cyber Security and Complex Software Systems Program](#), which focuses on the design and construction of software systems that meet required assurances for security, safety, reliability and performance.

Provided by Office of Naval Research

Citation: Shedding the fat: ONR explores ways to trim software bloat, improve security (2016, July 12) retrieved 23 April 2024 from <https://phys.org/news/2016-07-fat-onr-explores-ways-trim.html>

This document is subject to copyright. Apart from any fair dealing for the purpose of private study or research, no part may be reproduced without the written permission. The content is provided for information purposes only.