New program seeks to reveal backdoors and other hidden malicious functionality in commercial IT devices

December 3 2012

The scenario is one that information security experts dread: widespread dissemination of commercial technology that is secretly wired to function in unintended ways or even spy on its users. From this vantage

point, mobile phones, network routers, computer work stations and any other device hooked up to a network can provide a point of entry for an adversary.

For the Department of Defense this issue is even more of a concern now than ever before as DoD personnel rely on equipment bought in large quantities and built with components manufactured all over the world. DoD's growing dependence on the global supply chain makes device, software and firmware security an imperative. Backdoors, malicious software and other vulnerabilities unknown to the user could enable an adversary to use a device to accomplish a variety of harmful objectives, including the exfiltration of sensitive data and the sabotage of critical operations. Determining the security of every device DoD uses in a timely fashion is beyond current capabilities.

To address the threat of malicious code, DARPA is starting the Vetting Commodity IT Software and Firmware (VET) program to look for innovative, large-scale approaches to verifying the security and functionality of commodity IT devices (those commercial information technology devices bought by DoD) to ensure they are free of hidden backdoors and malicious functionality. On December 12th, DARPA will host a Proposers' Day in Arlington, Va. Here, participants will be briefed on the program and anticipated solicitation.

"DoD relies on millions of devices to bring network access and functionality to its users," said Tim Fraser, DARPA program manager. "Rigorously vetting software and firmware in each and every one of them is beyond our present capabilities, and the perception that this problem is simply unapproachable is widespread. The most significant output of the VET program will be a set of techniques, tools and demonstrations that will forever change this perception."

VET will attempt to address three technical challenges:

- Defining malice: Given a sample device, how can DoD analysts produce a prioritized checklist of software and firmware components to examine and broad classes of hidden malicious functionality to rule out?
- Confirming the absence of malice: Given a checklist of software and firmware components to examine and broad classes of hidden malicious functionality to rule out, how can DoD analysts demonstrate the absence of those broad classes of hidden malicious functionality?
- Examining equipment at scale: Given a means for DoD analysts to demonstrate the absence of broad classes of hidden malicious functionality in sample devices in the lab, how can this procedure scale to non-specialist technicians who must vet every individual new device used by DoD prior to deployment?

More information: go.usa.gov/gjEA

Provided by DARPA