Longitude149

Title: Can Darpa Fix the Cybersecurity 'Problem From Hell?'
Published: 05 Aug 2011
Author(s): Adam Rawnsley
Original Source: wired.com[1]

Can Darpa Fix the Cybersecurity 'Problem From Hell?'

There are computer security threats -- and then there are computer security nightmares. Put sabotaged circuits firmly in the second category. Last week, retired Gen. Michael Hayden, the former CIA and NSA chief, called the hazard of hacked hardware "the problem from hell."

"Frankly, it's not a problem that can be solved," he added. "This is a condition that you have to manage."

The Pentagon's top research division is trying, however. Over the past two months, Darpa, has awarded nine contracts totaling $49 million for its Integrity and Reliability of Integrated Circuits (IRIS) program to check for compromised chips. Seven companies and two universities received the awards.

The Defense Department has been worried about foreign adversaries tampering with its hardware for a while now. The Pentagon now buys 1 percent of all the world's integrated circuit production; America's defense community simply uses too many to monitor them all. In 2005, a Defense Science Board report warned that foreign adversaries could slip back doors into chips destined for installation in important military gear.

The hacked circuits, the report said, could be tweaked to malfunction early or provide a de facto kill switch to a weapon system.

The IRIS program builds off a previous Darpa chip-checking program called TRUST. TRUST uses imaging techniques like X-rays to compare chips against their complete design specifications. IRIS, however, is looking for ways to reverse engineer a chip and find out everything it does, even when the complete design specs aren't available.

The prospect of this kind of hacked hardware in the defense supply chain is linked to changes in chip-manufacturing processes. Globalization has shifted the map of where chips are built these days. Much of the production now takes place in countries like Taiwan, China, Japan and South Korea.

Different companies are also involved in the process, including those who design the chips and the foundries that manufacture them. The United States can't just trust the chip's designer, it needs to trust the company that manufactures it, too.

[1] https://www.wired.com/2011/08/problem-from-hell/

Iarpa, the intelligence community's answer to Darpa, has put forth another program to get around the supply-chain vulnerability. Trusted Integrated Circuits (TIC) tries to help the United States take advantage of foreign chip-manufacturing facilities.

TIC looks at techniques the government can use at foreign chip foundries to reduce the risk of malicious tampering, like conducting the less sensitive parts of chip production at foreign foundries.

How big a threat are hacked chips? The White House's 2009 Cyberspace Policy Review says "few documented examples exist of unambiguous, deliberate subversions." Some hints of maliciously fishy hardware have cropped up, though.

Greg Schaffer, Acting Deputy Undersecretary at the Department of Homeland Security's National Protection and Programs Directorate, was asked at a Congressional hearing last month if he knew of any examples of hacked hardware turning up. "I am aware of instances where that has happened" was his vague response.

Darpa's also getting more involved in software security, in addition to its hardware-hacking efforts. On Thursday it announced a new "Cyber Fast Track" program to speed the development of smaller cybersecurity projects to under a year.

###