



WHARTON AEROSPACE & DEFENSE REPORT

Your Knowledge Source on the Aerospace & Defense Industry

The Software Challenge: Balancing Costs and Security Risks

January 16, 2009

The Aegis Combat System, introduced in 1980, is the current standard in advanced command-and-control weapon systems using computers to track and destroy targets. The programming required for this precision system is quaint by today's standards: less than two million lines of code. (By comparison, MS-DOS 1.0 had about 4,000 lines of code, Windows NT 3.1 had about 4 million to five million lines in 1993, and Windows Vista has more than 50 million lines of code)

The F-22 aircraft — one of the most lethal systems in the U.S. arsenal — was introduced in 2005 and required approximately four million lines of code. The F-35 jet fighter, scheduled to enter service around 2010, will have 12 to 14 million lines of code.

The Future Combat System, which is planned for 2015, will require a whopping 16 to 18 million lines of custom code and about 60 million lines of commercial off-the-shelf (COTS), government-written code and open source code.

The trajectory is clear: Software now plays a pivotal role in the efficiency and might of American weapons systems, and the military's dependence on its software-driven arsenal and communications systems is irreversible. At the same time, no one organization — neither the Pentagon, defense contractors nor systems integrators — is capable of developing, implementing, verifying and maintaining the deluge of code. The costs associated with this work are also increasing the price tag for these modern systems.

"If software isn't a *major* part of the cost of weapons systems, then it's a very significant part of the cost," says Mark Kagan, a research manager at International Data Corporation's Government Insights unit. "You can build a frigate which costs \$500 million to buy, but the largest part of the expense would not be the hull or the weapons, it would be the hardware and software."

Supply, Cost Crunch Force Overseas Sourcing

To control costs and to meet production deadlines, U.S. defense contractors are increasingly outsourcing this work overseas.

This raises several prickly security issues. With so many lines of custom code, commercial off-the-shelf code, special code written by government programmers and open-source programming, how do you verify that errors — accidental or malignant — are not introduced by overseas developers?

Despite any risks, analysts note that defense contractors are under competitive pressure to cut costs and outsourcing software development overseas is a major option. "They are outsourcing and keeping their fingers crossed with respect to quality and malicious code content," says Sami Saydjari, the chief executive at Cyber Defense Agency, a company that provides strategic advice to the Department of Defense (DoD) about protecting critical infrastructure. "Many of them would like to have an inspection process for quality control, but I have not seen anybody come up with an ideal one that preserves the price effectiveness of outsourcing while maintaining the quality."

The Wharton Aerospace & Defense Report interviewed several experts in this field who offered concrete steps to minimize the dangers.

Staying Local

"The easiest way to avoid these problems might be to not use any offshore subcontractors," says Kagan, but he is quick to point out that the market forces make this an unrealistic choice. "The cost differential can be so great — an Indian subcontractor can do the work at a quarter of the cost of an American contractor."

Kagan notes that Indian companies might do labor-intensive work — like checking code line-by-line — which American companies might not consider. "So there's a balancing between security, cost and where to outsource."

A 2007 document produced by the DoD, "Report of the Defense Science Board Task Force on Mission Impact of Foreign Influence on DoD Software," recommends that all custom code written for systems deemed critical be developed by cleared U.S. citizens.

Tracking Product Development

Miscommunication can also lead to major problems. This is especially true when a company outsources to a new partner for the first time and finds that the complicated software it receives is filled with features that it did not ask for or is missing the features it required. "I have heard of a number of incidents in which companies that have outsourced ended up with systems that didn't function the way they were supposed to," says Saydjari.

To mitigate this problem, Saydjari suggests creating more formalized specifications for each requirement followed by regular tests to make sure both sides are on the same page and on track.

A more malicious problem could be that a worker at a foreign company inserts more than you want into the software, hiding a Trojan horse or virus that can be activated later to allow outsiders to take control of the system. Experts encourage organizations to use verification and quality assurance tools that can check for embedded threats. But these have limitations. "You have to train people to use [them] properly," says Kagan. "And these tools don't work in every case, because there might not be an application to check custom code. In that case, you have to have somebody go through it line-by-line by eyeball."

Yet, with millions of lines of code, the challenge could go beyond human ability to inspect.

Visiting the Workspace

A critical step in deciding whom to work with is to tour the facilities of the company that might develop your code and to scrutinize the security control measures, including who has access to the development process.

Partha Sarathy Guha Patra, who heads Wipro's aerospace and defense practice based in India, notes that former U.S. Under Secretary of Defense for Acquisition, Technology and Logistics Kenneth J. Krieg visited Wipro's facilities to "really understand" the layout of the environment and to see how it connects as a secure extension of the customer's own network.

"He could see that someone sitting in the U.S. could identify who is entering into a room, or logging into or logging off the network, or what changes that person was making to what file," says Patra. "From that perspective, it is important to win the confidence of your customer."

While none of these measures provides a silver bullet solution to all possible threats, they are a good starting point to create a secure working relationship with an offshore partner, according to analysts.