Mission Impact of Foreign Influence on DoD Software

Defense Science Board Task Force

The Defense Science Board task force assessed the Department of Defense's (DoD) dependence on software of foreign origin and the risks involved. The task force considered issues with supply chain management; techniques and tools to mitigate adversarial threats; software assurance within current DoD programs; and assurance standards within industry, academia, and government. This executive summary highlights the future U.S. ability to ensure and maintain a trusted supply of software to the DoD and the U.S. government. The full report states that there is no absolute guarantee that software can be sanitized of all vulnerabilities, intended or unintended, and recommends a suite of processes and mitigation strategies to reduce the risk of interrupted systems performance and ensure mission success.

Software has become the central ingredient of the information age, increasing productivity, facilitating the storage and transfer of information, and enabling functionality in almost every realm of human endeavor. However, as it improves the DoD capability, it increases the DoD's dependency. Each year the DoD depends more on software for its administration and for the planning and execution of its missions. This growing dependency is a source of weakness exacerbated by the mounting size, complexity and interconnectedness of its software programs. It is only a matter of time before an adversary exploits this weakness at a critical moment in history.

The software industry has become increasingly and irrevocably global. Much of the code is now written outside the United States, some in countries that may have interests inimical to those of the United States. The combination of the DoD's profound and growing dependence upon software and the expanding opportunity for adversaries to introduce malicious code into this software has led to a growing risk to the nation's defense.

A previous report of the Defense Science Board, "High Performance Microchip Supply," discussed a parallel evolution of the microchip industry and its potential impact on U.S. defense capabilities. The parallel is not exact because the microchip fabrication business requires increasingly large capital formation – a considerable barrier to entry by a lesser nation-state. Software development and production, by contrast, has a low investment threshold. It requires only talented people, who increasingly are found outside the United States.

The task force on microchip supply identified two areas of risk in the offshoring of fabrication facilities – that the United States could be denied access to the supply of chips and that there could be malicious modifications in these chips. Because software is so easily reproduced, the former risk is small. The latter risk of *malware*, however, is serious. It is this risk that is discussed at length in this report.

Software that the DoD acquires has been loosely categorized as:

- Commodity products – referred to as commercial off-the-shelf (COTS) software.
- General software developed by or for the U.S. government – referred to as government off-the-shelf software.
- Custom software – generally created for unique defense applications.

The U.S. government is obviously attracted by the first, COTS. It is produced for and sold in a highly competitive marketplace and its development costs are amortized across a large base of consumers. Its functionality continually expands in response to competitive market demands. It is, in a word, a bargain, but it is also most likely to be produced offshore and so presents the greater threat of malicious modification.

There are two distinct kinds of vulnerabilities in software. The first is the common *bug*, an unintentional defect or weakness in the code that opens the door to opportunistic exploitation. The DoD shares these vulnerabilities with all users. However, certain users are *high value targets*, such as the financial sector and the DoD. These high-value targets attract the *high-end* attackers. Moreover, the DoD also may be presumed to attract the most skilled and best-financed attackers – a nation-state adversary or its proxy. These high-end attackers will not be content to exploit opportunistic vulnerabilities which might be fixed and therefore unavailable at a critical juncture. Furthermore, they may seek to implant vulnerability for later exploitation. It is bad enough that this can be done remotely in the internetworked world, but worse when the malefactors are in the DoD's supply chain and are loyal to and working for an adversary nation-state – especially a nation-state that is producing the software that the U.S. government needs. The problem is serious, indeed. Such exploitable vulnerabilities may lie undetected until it is too late.

Unlike previous critical defense technologies which gave the U.S. an edge in the past, such as stealth, the strategic defense initiative, or nuclear weaponry, the U.S. is protected neither by technological secrets nor a high barrier of economic cost. Moreover, the consequences to U.S. defense capabilities could be even more severe than realized. Because of the high degree of interconnectedness of defense systems, penetration of one application could compromise many others.

In a perfect world there would be some automated means for detecting malicious code. Unfortunately, no such capability exists, and the trend is moving inexorably further from it as software becomes ever more complex and adversaries more skilled. Even if malicious code were discovered in advance, attributing it to a specific actor and/or knowing the intent of the actor may be problematic. Malicious code can resemble ordinary coding mistakes and malicious intent may be plausibly denied. The inability to hold an individual accountable weakens deterrence mechanisms, such as the threat of criminal charges, or even separation of the individual or entity from the supply chain.

Task Force Conclusion

The DoD faces a difficult quandary in its software purchases in applying intelligent risk management, trading off the attractive economics of COTS and of custom code written offshore against the risks of encountering malware that could seriously

jeopardize future defense missions. The current systems designs, assurance methodologies, acquisition procedures, and knowledge of adversarial capabilities and intentions are inadequate to the magnitude of the threat.

Task Force Findings

The Industry Situation

The software industry has become increasingly global as suppliers seek lower cost employees, access to a larger talent base, cultures conducive to highly structured processes, and round-the-clock operation. The issue of foreign influence is only one of degree, because many companies develop code in multiple geographic locations and may embed code from other vendors, code from open source developers, or even code of unknown provenance.

While the United States still has preeminence in computer science, Asia is rapidly gaining. The United States retains a pool of talented computer scientists and engineers, but the natural tendency of the industry is to seek the lowest cost supply of talent. In recent years, that has been primarily in India, while China and Russia are on the rise.

DoD's Dependence on Software

In the DoD, the transformational effects of information technology (IT), joined with a culture of information sharing, called Net-Centricity, constitute a powerful force multiplier. DoD has become increasingly dependent for mission-critical functionality upon highly interconnected, globally sourced, information technology of dramatically varying quality, reliability, and trustworthiness.

Software Vulnerabilities

The majority of software used in the DoD are COTS products. Although the DoD takes advantage of the functionality and inexpensive pricing enabled by the huge market, this code has many weaknesses that are exploitable by even moderately capable hackers who have been the beneficiaries of a culture that has produced an evolution of widely disseminated and powerful tools for system intrusion.

The DoD does not fully know when or where intruders may have already gained access to existing computing and communications systems. The Moonlight Maze activities, which are classified and thus not detailed here, and numerous other data points demonstrate that the U.S. government, and specifically the DoD computing systems, is a constant target of foreign exploitation.

The Threat of the Nation-State Adversary

In dealing with a nation-state adversary, the level of threat rises far above that posed by hackers. It can be assumed that the technological capability to craft actionable malicious code mirrors that of the United States' own best computer scientists. Means and opportunity are present throughout the supply chain and life cycle of software development. While code developed in the United States is not immune from risk, the opportunity for an adversary is greatly enhanced by globalization.

A sophisticated adversary would have three possible aims in the exploitation of existing or planted software vulnerabilities: denial of service, stealing of information, and malicious modification of information. The outcome of any of these would also be accompanied by a loss of confidence in the DoD's essential systems.

"In a perfect world there would be some automated means for detecting malicious code. Unfortunately, no such capability exists, and the trend is moving inexorably further from it as software becomes even more complex and adversaries more skilled."

Awareness of the Software Assurance Threat and Risk

The DoD's defensive posture remains inadequately informed of the sophisticated capabilities of nation-state adversaries to exploit globally sourced, ubiquitously interconnected, COTS hardware and software within DoD critical systems. Similarly, decision makers are inadequately informed regarding the potential consequences of system subversion, and the value of mitigating that risk.

The intelligence community does not adequately collect and disseminate intelligence regarding the intents and capabilities of nation-state adversaries to attack and subvert DoD systems and networks through supply chain exploitations, or through other sophisticated techniques.

The DoD does not consistently or adequately analyze and incorporate into its acquisition decisions what supply chain threat information is available.

Status of Software Assurance in the DoD

Software deployed across the DoD continues to contain numerous vulnerabilities and weak information security design characteristics. The DoD and its industry partners spend considerable resources on patch management while gaining only limited improvement in defensive posture.

The evidence gathered during this study was insufficient to quantify the extent to which awareness and protection against the system assurance problem has permeated DoD systems and networks. The panel did, however, identify considerable variation in the extent to which the systems assurance problem is impacting next-generation DoD systems. That impact ranges from extensive with the introduction of internetworked COTS and open source IT into the Army's Future Combat System program, to only slight in the United States Air Force F-22 program.

The DoD defensive efforts, implemented largely through decentralized execution, are difficult to synchronize to achieve a coordinated enterprise effect. The DoD has not effectively allocated assurance resources to address the systems assurance problem, nor has it designed its systems and networks to mitigate this problem in the face of the capabilities of nation-state adversaries.

The primary process relied upon by the DoD for evaluation of the assurance of commercial products today is the Common Criteria (CC) evaluation process. The task force believes that CC is presently inadequate to sufficiently raise the trustworthiness of software products for the DoD. This is particularly true at Evaluation Assurance Level 4 (EAL4) and below, where penetration testing is not performed. Nonetheless, CC evaluation is an international program, well established, and not easy to change.

Ongoing Efforts in Software Assurance

Software assurance is receiving attention at a number of federal agencies and laboratories, including the DoD, National Security Agency (NSA), National Institute of Standards and Technology, and Department of Homeland Security (DHS). Within the DoD, a Software Assurance Tiger Team has been studying

the problem and has developed a comprehensive strategy for managing risk through system engineering, source selection, design, production, and test. The key element of risk management in this strategy is the prioritization of criticality among system components and subcomponents, with special procedures and attention placed on the system components determined to be most critical to mission success.

Supplier Trustworthiness Considerations
It is not currently DoD policy to require any program – even those deemed critical by dint of a Mission Assurance Category I status – to conduct a counterintelligence review of its major suppliers unless classified information is involved. Supplier trustworthiness enters into existing DoD acquisition processes primarily for protection of classified information and for research technology protection. From a systems assurance perspective, supplier trustworthiness should consider adversarial control and influence of the business or engineering processes of the supplier, as well as the ability of the business and engineering processes to prevent outside penetration.

Finding Malicious Code
The problem of detecting vulnerabilities is deeply complex, and there is no silver bullet on the horizon. Once malicious code has been implanted by a capable adversary, it is unlikely to be detected by subsequent testing. A number of software tools have been developed commercially to test code for vulnerabilities, and these tools have been improving rapidly in recent years. Current tools find about one-third of the bugs prior to deployment that are ever found subsequently, and the rate of false positives is about equal to that of true positives. However, it is the opinion of the task force that unless a major breakthrough occurs, it is unlikely that any tool in the foreseeable future will find more than half of the suspect code. Moreover, it can be assumed that the adversary has the same tools; therefore, it is likely the malicious code would be constructed to pass undetected by these tools.

The task force believes that the academic curriculum in computer science does not stress adequately practices for quality and security, and that many programmers do not have a defensive mindset. While many vendors methodically check and test code, they are looking for unintentional defects, rather than malicious alterations.

Government Access to Source Code
It is tempting to consider having the United States government take the source code of a commercial product and run its own vulnerability assessment tools against it. However, there are a number of legal, ethical, and economic barriers that make this an unattractive proposition, particularly from the point of view of the vendor. License agreements forbid reverse engineering of source code, vendors worry about the loss of intellectual property, and perhaps most importantly, they worry about the cost of supporting the actions and findings of a team of outsiders not familiar with the design and implementation of such hugely complex programs. Some of these worries are lessened when the testing is done by an independent laboratory.

"There is a natural tension between the U.S. government's need to know the security worthiness of what they procure and a vendor's need to avoid disclosing particular vulnerabilities."

Conclusion
All of the considerations just listed seem to point to an intractable problem. The nation's defense is dependent upon software that is growing exponentially in size and complexity, and an increasing percentage of this software is being written offshore within easy reach of potential adversaries. That software presents a tempting target for a nation-state adversary. Malicious code could be introduced inexpensively, would be almost impossible to detect, and could be used later to get access to defense systems in order to deny service, to steal information, or to modify critical data. Even if the malware were to be discovered, attribution and intent would be difficult to prove, so the risk for the attacker would be small.

Against this backdrop of potential disaster, practical experience and belief paint a picture of aggravating and continuous software problems, but not ones that are lethal. However, there are some systems on which, to varying degrees, life depends (e.g., power, health). In this sense, DoD systems are among the most critical because their national security mission is often measured in fatalities, and failures that would be innocuous in another context can be lethal and lead to mission failure.

If the attacker cannot be deterred and its malware cannot be found, what is to be done to provide assurance that DoD software will perform in mission-critical situations? Although there never will be an absolute guarantee, software assurance is really not about absolute guarantees but rather intelligent risk management. The risk of vulnerable software can be managed through a suite of processes and mitigation strategies detailed in the Task Force recommendations; this risk can be weighed against the attractive economics and enhanced capabilities of mass-produced, international software.

Task Force Recommendations

Acquisition of COTS and Foreign Software
DoD should continue to procure from, encourage and leverage the largest possible global competitive marketplace consistent with national security.

The DoD must intelligently manage economics and risk. For many applications the inexpensive functionality and ubiquitous compatibility of COTS software make it the right choice. In acquiring custom software the increased risk inherent in software written offshore may sometimes be worth the considerable cost savings. The task force recommends that critical system components be developed only by cleared U.S. citizens.

Increase U.S. Insight Into Capabilities and Intentions of Adversaries
The intelligence community should be tasked to collect and disseminate intelligence regarding the intents and capabilities of adversaries, particularly nation-state adversaries, to attack and subvert DoD systems and networks through supply chain exploitations, or through other sophisticated techniques.

DoD should increase knowledge and awareness among its cyber-defense and acquisition communities of the capabilities and intent of nation-state adversaries.

Offensive Strategies Can Complement Defensive Strategies
The United States government should link cyber defensive and offensive opera-

tions to its broader national deterrence strategies, communications and operations, treating adversarial cyber operations that damage United States information systems and networks as events warranting a balanced, full-spectrum response.

System Engineering and Architecture for Assurance

The DoD should allocate assurance resources among acquisition programs at the architecture level based upon mission impact of system failure. The task force endorses the strategy and methods to accomplish this as developed by the DoD Software Assurance Tiger Team and validated by the Committee on National Security Systems (CNSS) Global IT Working Group.

The DoD cannot cost effectively achieve a uniformly high degree of assurance for all the functionality it uses across many and varied mission activities. Allocating criticality of function levies a requirement for assurance of that function and also of those functions that defend it. Systems identified as critical must then allocate criticality at the subsystem and assembly level.

To properly allocate scarce assurance resources, the DoD must allocate criticality at the system-of-systems and enterprise architecture level. This analysis should occur early within the lifecycle, and should render a prioritization decision no later than Acquisition Milestone A to allow programs of record to appropriately respond to their criticality.

Improve the Quality of DoD Software

The DoD can effectively raise the *signal-to-noise ratio* against software attacks by raising the overall quality of the software it acquires. If there were fewer unintentional bugs in software, the visibility of deliberate malware would be increased. While general improvements in information assurance will not, per se, prevent a determined attacker from corrupting the software supply chain, there are several compelling benefits in improving the overall assurance/security worthiness of COTS.

A sophisticated adversary would have to work harder to introduce an exploitable vulnerability instead, as is currently the case, of relying upon the plausible deniability of a common programming error to avoid attribution of malicious intent. Furthermore, a sophisticated adversary would have less confidence that its malware would remain undetected, invisible in a world containing far fewer distracting vulnerabilities. That uncertainty could be a deterrent in itself.

Improve Tools and Technology for Assurance

Improve Trusted Computing Group (TCG) Technologies

The TCG initiatives, centered on the Trusted Platform Module (TPM), provide a means for containing intrusions into separated information domains. Each chipset that implements the TPM embeds a unique identifier. Cryptologic verification of this identity is required when access to system assets is requested. TPM may help ensure that only approved and signed code is run, thus reducing the risk of unapproved code being installed.

The NSA and others have identified a number of improvements and complementary practices that would strengthen TCG-compliant systems, including privacy-preserving attestation, virtualization, and architectures that provide richer software assurance measurement and monitoring capabilities.

Improve Effectiveness of Common Criteria

Currently, the official DoD-wide evaluation/validation scheme is the National Information Assurance Partnership based upon the CC. The reality today is that it would be far easier and more effective to improve CC than to invent a new scheme specific to the DoD or to DHS.

A number of ways to strengthen CC are discussed in the Recommendations section of this report. Among these suggestions are crediting vendors for the effective use of better development processes, including the use of automated vulnerability reduction tools and automated tools for vulnerability analysis during EAL4 and below. Validation schemes should also reduce artificial artifact creation and rely upon artifacts that are generated by the development process.

Improve Usefulness of Assurance Metrics

There is a natural tension between the United States government's need to know the security worthiness of what they procure and a vendor's need to avoid disclosing particular vulnerabilities. One way to satisfy both needs would be to develop a weighted index of the security worthiness of software. A weighted score could be generated via testing based on some combination of the utility of the tools themselves, the amount of code coverage of the tools, and the test results against a particular product. The entire development process should also be evaluated.

More Knowledgeable Acquisition of DoD Software

The DoD should implement a scalable supplier assurance process to assure that critical suppliers are trustworthy. No product evaluation regime in effect today provides insight into a vendor's real development processes and their effectiveness at producing secure and trustworthy software – so the software assurance challenge for the DoD is to define an evaluation regime that is capable of reviewing vendors actual development processes and rendering a judgment about their ability to produce assured software.

The DoD acquisition process should require that products possess assurance matching the criticality of the function delivered. Furthermore, the DoD should require that all components should be supplied by suppliers of commensurate trustworthiness, and in particular, that all custom code written for systems deemed critical be developed by cleared U.S. personnel.

The collective buying power of the United States government is such that it can force change on its suppliers to a degree no other market sector can reasonably do. The DoD, working in collaboration with the Office of Management and Budget, DHS, and other federal agencies, can help to change the market dynamic through both positive and negative incentives so that they get better quality software, and to make better risk-based and *total cost*-based acquisitions.

Research and Development in Software Assurance

The DoD should establish and fund a comprehensive science and technology strategy as well as programs to advance the state-of-the-art in vulnerability detection and mitigation within software and hardware. The goals of the classified and unclassified research and development investments in assurance should be to develop the technology to effectively take accidental vulnerabilities out of systems development and to improve TCG technologies in order to bound most risks of intentionally planted software. This program should monitor what markets are delivering, identify gaps between what the market is delivering and what the DoD needs, and fill the gap.◆

For more information on the Defense Science Board Task Force findings, go to <www.acq.osd.mil/dsb> and search under "Reports."