Raising the Bar on Cybersecurity and Acquisition

Michael L. Papay
Frank J. Cilluffo
Sharon L. Cardash

October 2014

Michael L. Papay, Ph.D., is Northrop Grumman's Vice President and Chief Information Security Officer. Frank J. Cilluffo is Director of the George Washington University Cybersecurity Initiative and GW's Homeland Security Policy Institute (HSPI). Sharon L. Cardash is Associate Director of HSPI and a Founding Member of GW's Cyber Center for National & Economic Security.

*Cybersecurity at the George Washington University is anchored by the **Cybersecurity Initiative**, launched in 2012 and managed through the Homeland Security Policy Institute. The Cybersecurity Initiative is one of the important cross-disciplinary initiatives emerging from Vision 2021, the university's strategic plan. With strong ties from Capitol Hill to Silicon Valley to Wall Street, GW is a convening force for discussion and consensus building on the major issues in cybersecurity and national security, a "one stop shop" for all things cyber-related that takes a multifaceted approach to a complex discipline. Opinions expressed in this Issue Brief are those of the authors alone. Comments should be directed to cyber@gwu.edu.*

***Northrop Grumman** is a leading global security company providing innovative systems, products and solutions in unmanned systems, cyber, C4ISR, and logistics and modernization to government and commercial customers worldwide. Please visit www.northropgrumman.com for more information.*

Introduction

Consider the following three scenarios:

Scenario 1: An American UAV falls into foreign hands over hostile territory. Engineers there seek to reverse engineer the design. With help from another government, the adversary comes into possession of the blueprints for highly advanced US military technology that can be used to secure profound military and strategic advantage. In little more than the blink of an eye, US defense systems that took decades to develop are compromised and, worse yet, leveraged by our adversaries while at the same time, the US military and intelligence communities are deprived of a key capability.

Scenario 2: The navigation system of a multi-million dollar private yacht, which relies on the Global Positioning System (GPS), is hijacked remotely by hackers who cause the vessel to veer off course. The cyber intruders manage to spoof the yacht's GPS coordinates, by generating false signals deemed credible by on-board mechanisms, thereby evading the threat sensors that reside in the ship's command room. Fortunately, the perpetrators in this case are university researchers engaging in scholarly inquiry designed to further the public interest.[1] The next time, however, the owner and occupants of the vessel may not be so lucky.

Scenario 3: On a busy highway in Miami a member of a drug trafficking organization spots a rival that he wants to neutralize. A serious car crash would do the trick. Leaving essentially no fingerprints, he hacks into the rival's vehicle and disrupts its communications and signaling mechanism. The car now thinks it has a flat tire and stops abruptly. Then, the vehicle-to-vehicle messaging system (that a few years from now will connect cars and generate automatic responses), causes all those behind the targeted car to come to an abrupt stop, creating a huge pileup. Dozens are hurt and the target is left paralyzed due to neck injuries.

Sound farfetched? In fact, the first two scenarios have already materialized and the third is possible soon, as the Internet of Things continues to evolve and introduces a new dimension of connectivity in which everything from cars to pacemakers to refrigerators can be manipulated electronically and remotely.

These extraordinary developments have an upside and a downside that are both equally profound. On the one hand, such technological advances hold the potential to make everything from lifesaving healthcare to mundane daily tasks faster, easier and more widely available than ever before. On the other hand, any significant vulnerabilities in these advances could be exploited, unless we take the time, effort and investment to bake in security at the front end.

Embedding security into the design process is all the more important for defense-related matters that form the cornerstone of US national and economic security. Yet Department of Defense (DOD) business (operations, platforms, programs, etc.) cannot be hived off from commercial off-the-shelf technology or the Internet of Things. Just like the rest of society, the DOD makes use of such devices. The critical

[1] "UT Austin Researchers Successfully Spoof an $80 million Yacht at Sea," (July 29, 2013), http://www.utexas.edu/news/2013/07/29/ut-austin-researchers-successfully-spoof-an-80-million-yacht-at-sea/

question, therefore, is what can the DOD do to protect itself and its missions insofar as cyber vulnerabilities are concerned?

Acquisition, Components and Cybersecurity: Bits & Bytes Can Bite

One of the most important challenges that DOD will face in the next 5 years centers on extending its cybersecurity experience and capabilities to battlefield systems. Critical warfighting capabilities are today reliant upon software-intensive and networked systems, with hundreds of suppliers involved. Yet manufacturing and supply chains may be exploited remotely, by actors who are not part of core DOD entities, and may seriously undermine confidence in US defense systems.

The threat spectrum of hostile actors who seek to gain control of defense systems through the supply chain includes nation-states, terrorists, and criminals. These adversaries aim to stymie US capabilities. In other words, they seek to steal US plans for next-generation aircraft, satellites and the like, in order to study the designs and figure out how best to attack them using cyber capabilities. Access to US plans also allows the adversary to identify vulnerabilities that can be exploited through conventional means, and saves our opponents the money and effort they would otherwise need to dedicate to the development of their own weapons as well as countermeasures. While building a large war chest for our opponents' military investment, economic espionage that supports business advantages for our adversaries damages the US economy. Protecting the battlefield in this day and age thus means protecting technology, components, and information. Failure to do so will compromise the effectiveness of our weapons platforms and systems. Though we know we need to develop a robust security posture, the path to that goal is extensive and ever-evolving. The power to travel further down that road, however, lies in the acquisition community, particularly by putting in place the necessary protections for mission-critical elements.

To some extent, the challenge lies in practice and implementation, since Department of Defense instructions on the subject already exist.[2] With regard to protecting technology and information, the relevant governing instructions seek to keep in safe hands the secret and the critical, respectively. For components, the focus of the Instruction is on keeping out the malicious. The means and mechanisms for achieving this last objective (as set out in DODI 5200.44) include the application of scientific and engineering principles to identify security vulnerabilities and minimize the associated risks; intelligence analysis to inform the risk management process; and countermeasures such as secure design patterns, software assurance, and supply chain risk management. Placed in broader context, the Instruction is designed to implement DOD's strategy for Trusted Systems and Networks.[3]

---

[2] See generally Interim Department of Defense Instruction (DODI) 5000.02. Re: Technology, see DODI 5200.39 – Change 1, dated December 2010. Re: Components, see DODI 5200.44. Re: Information, see DODI 8500 Series and, in particular, DODI 8500.01E and DODI 8582.01.

[3] Kristen Baldwin, Principal Deputy, Office of the Deputy Assistant Secretary of Defense for Systems Engineering, "DoD Trusted Systems and Networks (TSN) Update," Presentation to NDIA Systems Engineering Division Meeting (April 17, 2013), http://www.ndia.org/Divisions/Divisions/SystemsEngineering/Documents/Past%20Meetings/April%2017%202013%20Div%20meeting/03A%202013_04_17_Baldwin_NDIA-SE-Division-Mtg_Final.pdf

If the answer to the question "why does it matter?" is clear and compelling, and if the pathway to the goal is specified in DOD instructions, then why are we not doing what needs to be done to protect components from a cybersecurity perspective? The recent regulatory development, the May 2014 Defense Federal Acquisition Regulation Supplement (DFARS) concerning the detection and avoidance of counterfeit electronic parts[4], is assuredly a step in the right direction; though as always, the rubber will meet the road primarily in the implementation phase. The DFARS rule is one piece of the puzzle and aims to address a specific vulnerability. In addition, our systems—taken collectively—must be architected to prevent and detect cyber-attacks more broadly. Regarding other important steps not yet taken, likely there are multiple reasons as to why, such as the cost and time involved plus other competing demands upon those charged with implementation. Current training efforts also may be inadequate, resulting in a lack of understanding of the threat. Frankly, however, the why matters less than the fix—the problem just needs to be addressed as soon as possible. The good news is that there are plenty of solid ideas as to how.

Addressing the Vulnerability: Educate, Engineer, Evangelize

Where do we go from here? The first step is to raise the level of education and awareness about the challenge and its pressing nature. Training on topics such as secure architecture and secure coding for relevant personnel in place, and for the rising cybersecurity professionals who are still in college, is one important element of the remedy. Curriculum changes alone, however, will not get us to where we need to be. Leadership and a dedicated effort at the highest levels to instill a culture of cybersecurity, both widely and deeply, are also required. To take a page (or at least a term) from the Silicon Valley playbook, we must evangelize.

The task of modifying the mindset that secure systems, which take extra time and money to build, are essential (even if the customer has not specifically asked for that feature) is the quintessential uphill battle; but we need to take that hill. Put differently, cybersecurity must be applied to and embedded in information technology, engineering and systems architecture. Engineering itself thus becomes, among many other things, an exercise in design which includes analysis of security requirements and building the architecture (such as intrusion detection systems) to meet those requirements.

Properly understood, this exercise in design is an enormous challenge that requires creativity and brainpower—the very same principles that animate ethical or "white hat" hacking competitions, as well as Silicon Valley's energy and appetite for tackling the world's most wicked problems. Cast in the right terms and conveyed to the right audience, then, it may be ambitious (but certainly not folly) to believe that engineering secure technologies and systems may come to be seen as a very "cool" thing to do. Indeed, our nation would do well to adopt that mindset and the sooner the better.

[4] http://www.gpo.gov/fdsys/pkg/FR-2014-05-06/pdf/2014-10326.pdf

From DOD to Critical Infrastructure and the Internet of Things: Securing our Foundations

Secure design ought not to be of exclusive concern to DOD. Consider our critical infrastructure systems such as in the energy sector. Are we approaching with sufficient vigilance the task of embedding cybersecurity into the design of our facilities in key critical infrastructure sectors? Or, is the intellectual property that powers operations and innovations within these sub-sectors at serious risk? Similarly, consider the potential consequences of compromise of our cars or even our home appliances. A hacked vehicle could result in loss of life or limb; and a compromised fridge (or smartphone) could serve as an entrée to manipulate other networked devices and data. To the extent that we are not as focused as we could be on securing these connections from the outset, we are doing ourselves a disservice. Unless we make an even broader, concerted and sustained effort, to embed cybersecurity into the devices that constitute part of the Internet of Things (IOT) we will be repeating the same mistake over and over, expecting a different result. The case is all the more compelling because cybersecurity can and should be enhanced in an affordable manner that does not simply add costs to the end consumer. This could be accomplished by starting early in the design process and continuing through product testing.

In turning our attention to the Internet of Things, we recognize the risk of trying to boil the ocean in a single go. Indeed, our primary and immediate concern is to draw attention to the cybersecurity of components that figure into DOD's acquisition process. However, it is important to note that even DOD's missions and full-spectrum operations intersect meaningfully with the IOT. The Department is not a watertight compartment that functions in complete isolation from the broader commercial ecosystem. To the contrary and as pointed out in recent Congressional testimony:

> The Department relies heavily on customized and commercial off-the-shelf (COTS) computers, communications equipment, integrated circuits (ICs), application software, and other information communications technology (ICT) to stay on the cutting edge of technology development and fulfill mission-critical operations. With increasing frequency, the Department and its commercial supplier base rely on foreign companies to produce the most advanced technology solutions.[5]

Having said that, it is equally important to note the existence of guidelines for DOD mission/operational network connectivity with commercial IOT enabled devices. Once again, though, implementation is everything; guidance in and of itself is merely words on a page.

The good news is that the broader message about cybersecurity is getting out. Popular entertainment such as the TV show "24" and the video game "Watch Dogs" are raising awareness about the perils and havoc that may be caused by cyber means. On "24", viewers witness (spoiler alert) the portrayed adversary hacking into the US unmanned fleet and launching attacks on London. Likewise in "Watch Dogs," which was Ubisoft's best-selling game released in June 2014[6], the protagonist strides menacingly through the

[5] Statement by Mitchell Komaroff, Director, Trusted Mission Systems and Networks, Office of the Department of Defense Chief Information Officer, "IT Supply Chain: Review of Government and Industry Efforts" (March 27, 2012), Before the House Energy and Commerce Committee, Subcommittee on Oversight and Investigations, at page 3.

[6] http://www.technologytell.com/gaming/129405/watch-dogs-now-ubisofts-bestselling-game/

streets, contemplating controlling trains, jamming communications and traffic lights, etc., all with the mindset that "hacking is our weapon." It's a "hacktion-adventure" game: "Players are offered any number of ways to hijack the infrastructure of an entire city, dynamically affecting more moving parts than even the fittest, most well-armed avatar piloting the world's finest combat-ready helicopter ever could."[7]

It may be a game but the premise is deadly serious. As in the fictional but not farfetched Scenario 3 above (at page one), the underpinning notion that connectivity gives rise to new sources of power that may be exercised by friend and foe alike, serves to reinforce our overarching argument—that embedding cybersecurity into the design phase (at the hardware, software and interface protocol level) is an imperative that must be treated as such. While there is no limit on the various creative ways that we may get to goal in this area, one prudent and relatively simple course would be for all IOT enabled devices to have shutoff modes that provide users optional connectivity choices that default to off upon shipping, and self-patch themselves upon activation.

Conclusion

If there is a single takeaway from this paper, it is that you don't have true, reliable capability if you don't have security. Fortunately, there are some encouraging examples of individuals and entities taking action to incorporate and enhance cybersecurity before harms materialize. One such example would be the recent Federal Aviation Administration (FAA) order "requiring Boeing to modify the technology aboard 737 jetliners" in order to safeguard those planes from hackers seeking to exploit "the network configuration on these models [which] allows increased connectivity with external networks, such as passenger entertainment and information services…".[8]

As mentioned above, however, our priority in the short-term is the defense realm and in particular, how best to bring the acquisition of components into alignment with a robust cybersecurity posture. With this in mind, we offer the following specific and granular recommendations for action, in addition to the ideas suggested above:

Action Recommendations for the Department of Defense

- The Department of Defense should undertake an internal review of its critical weapons systems and their cybersecurity effectiveness in relation to both known and anticipated threats. The goal is

[7] Evan Shamoon, "Hack the Block: The Success of `Watch Dogs', " *Rolling Stone* (June 16, 2014), http://www.rollingstone.com/culture/news/hack-the-block-the-success-of-watch-dogs-20140616#ixzz34pqX0yoU

[8] Amanda Vicinanzo, "FAA Orders Boeing To Protect 737s From Hackers," *HSToday.US* (June 13, 2014), http://www.hstoday.us/briefings/industry-news/single-article/faa-orders-boeing-to-protect-737s-from-hackers/f52534c49760584b58f8ca9e317f9141.html; see also: Rule by the FAA, "Special Conditions: The Boeing Company, Models 737-700, -700C, -800, -900ER, -7, -8, and -9 Series Airplanes; Isolation or Airplane Electronic System Security Protection From Unauthorized Internal Access," (June 6, 2014), ["This may allow the exploitation of network security vulnerabilities resulting in intentional or unintentional destruction, disruption, degradation, or exploitation of data and systems critical to the safety and maintenance of the airplane, which could result in unsafe conditions for the airplane and its occupants"], https://www.federalregister.gov/articles/2014/06/06/2014-13245/special-conditions-the-boeing-company-models-737-700--700c--800--900er--7--8-and--9-series-airplanes.

to acquire and adopt secure technologies, components, systems, etc., in a manner that reflects a careful appreciation of risk-based cyber considerations.

- The voluntary standards and best practices contained in the National Institute of Standards and Technology (NIST)'s Framework for Improving Critical Infrastructure Cybersecurity represents a good step forward, and adopting the vernacular as a way to communicate the criticality of security controls to the acquisition community is an excellent step.

- The Defense Science Board (DSB) should design and undertake a study to determine how to measure the balance between security and capability, in order to incorporate cybersecurity policy into the acquisition process in a scientific manner that eliminates guesswork. This study—a security/capability tradeoffs analysis—could and should be followed by related efforts directed towards the civilian/commercial context (see below the Recommendations for the Private Sector).

Action Recommendations for Congress

- In tandem with the internal DOD review referenced above, Congress should support and enable the conduct of an audit, carried out by the Government Accountability Office (GAO), centered on critical US weapons systems and their cybersecurity effectiveness against threats both known and anticipated.

- Work to pass aspects of cybersecurity legislation that have broad, bipartisan support within Congress, including reform of the Federal Information Security Management Act (FISMA) and legislation that removes real or perceived barriers to information sharing between entities in the public and private sector.

Action Recommendations for the Private Sector

- The National Academy of Engineering (NAE) should design and undertake a study to determine how to measure the balance between security and capability, in order to incorporate cybersecurity policy into the commercial design process in a scientific manner that eliminates guess work. This study—a security/capability tradeoffs analysis, applicable to the many and varied devices that constitute the Internet of Things—should be performed in complement to the DSB study focused on the defense sector (referenced above).

- Private sector entities should carefully review and adopt where appropriate the voluntary standards and best practices contained in the National Institute of Standards and Technology (NIST)'s Framework for Improving Critical Infrastructure Cybersecurity.

Action Recommendations for All Stakeholders

- All stakeholders should commit to better their understanding of what threats are on the horizon, and make that information available to others—including those in the defense acquisition system, so as to facilitate risk management and mitigation. Our operating presumption should be that a compromise will occur—that it is a matter of when, not if. Accordingly, all stakeholders should seek to determine how to build resilience and maintain functionality, even if attacked.[9]

- All stakeholders should make available more resources for training in the area of cybersecurity as it pertains to the acquisition and secure design processes. Even during a period of significant budgetary pressure such as the present, training of this type should be a genuine priority; and if undertaken widely, will have the added benefit of protecting and generating economic gains (for example, by means of safeguarding US intellectual property, blueprints for innovation, etc.).

###

[9] This effort could and should build upon the studies recently conducted by the NAE on the subject of resilience.