leidos

Cyber Hardening Legacy Weapons Systems

The United States has been confronting a growing threat to its defense.

Many of the nation's missiles and other weapons are legacy systems developed decades ago. At the time, engineers had no way of envisioning today's highly networked computing environments. The result is that these crucial weapons systems are now potentially vulnerable to cyber-attacks. The solution is to cyber harden the weapons to defend against adversaries' efforts to disable them, or possibly even manipulate them remotely.

Since the 1970s, Dynetics, a wholly-owned subsidiary of Leidos, has focused on defense threat systems analysis to discover how weapon systems can be exploited remotely and how to protect against that exploitation. A key approach is reverse engineering weapons systems to understand exactly how they function, even with little or no access to the weapons themselves or the computer processors and source code that control them.

THE LIMITS OF OBSCURITY AND AIR GAPPING

The processors and software that run critical weapons systems are, in many cases, legacy technology more than three decades old. And that's despite the fact that computing hardware and software have advanced exponentially over that time. It may seem surprising that these all-important weapons components haven't been updated, especially considering what's at stake. But there's a reason: Replacing them all would be a slow, massive, costly process, and one that might even risk a severe disruption in our national defense.

It's not that the legacy weapons software doesn't work well. It does. It's that these systems weren't designed to fend off contemporary cyber threats. Adversaries have had up to thirty years to decipher these weapons systems' cyber vulnerabilities and develop increasingly advanced ways to exploit them.

For a long time, weapons software was protected from cyberattacks through the principle of "security through obscurity," where basic details about the weapon systems, including their designs and locations, were closely guarded secrets. How do you attack something when you don't know what or where it is? After so long, we have to assume much of that information has ended up in the hands of potential attackers.

There was yet another layer of defense that used to work quite well. Namely, weapons systems were "air-gapped," meaning they had no physical data connection to the outside world, such as communications cables that tied computers to external networks. But with today's ubiquitous Wi-Fi and Bluetooth connectivity, physical connections have become irrelevant. Those wireless connections don't have to be built into the weapons to cause a problem. If any of the systems or personnel surrounding the weapons have wireless connections to the outside world, the weapons themselves become vulnerable. Isolating all those systems and personnel from wireless connectivity could prove difficult. That can leave hidden cyber-pathways open. Network firewalls designed to detect and repel cyber-attacks don't offer enough protection because adversaries assemble vast teams of highly skilled hackers whose lives are dedicated to getting around firewalls.

But the problem is even more extensive than that. All electronic devices emit electromagnetic signals, and sensors such as camera chips and electromechanical components such as cooling fans, can be especially noisy. This electronic noise can beam out critical clues to the computer processing activity in a weapons system. **Numerous academic papers** have already documented **the wealth of cyber information that can be gleaned** from **picking up these signals**. They have even proven that these electronic-noise pathways can be used to attack the system.

BOLTING ON PROTECTION

Because the costs and downtime of replacing or updating the processors and software controlling legacy weapons systems can be so high, defenders have to examine other options to protect them. One good way to do it is to "bolt on" cyber hardening. That is, engineers add additional software and hardware protections outside and around the systems' existing software and hardware, without needing to heavily modify what's already in place.

But bolting on protection comes with its own significant challenges. Sensitive weapon system components are so closely guarded that the components themselves and all details about them have to be kept secret from the very people charged with protecting them. It's just too risky to allow information about the inner workings of "exquisite" weapons systems—low-density, high-impact weapons—to circulate in any form outside of a tiny circle.

That's why starting decades ago, Dynetics developed a core competence of reverse engineering these systems. Armed with knowledge about what the system does and how it operates, Dynetics experts can figure out enough about the underlying hardware and software to protect them.

To help with reverse engineering, Dynetics has developed an extensive library of the designs and vulnerabilities of weapon systems processing, memory, and software components. That enables engineers to figure out precisely what they're protecting down to the bit level and derive the system's software source code, and put together an accurate hardware and software simulation of that system. At that point, Dynetics can perform a range of penetration testing and analysis procedures on the simulation and be fairly certain that the results closely match the actual weapons components. Then that simulation is used to design and test the needed hardware and code that will be bolted on to the real components.

A NEED TO PRIORITIZE

Countless weapons of all different types need additional cyber-defense, or will at some point. What's more, each of them consists of multiple components, and each of those parts comes with a long list of potential vulnerabilities. Even protecting a single component against a single vulnerability can be a significant project. Fully defending every single element of a weapons system against every single vulnerability would take far too long, cost far too much, and require far too many experts. That means it's critical to figure out which vulnerabilities of which elements need to be made a top priority.

Dynetics relies on a proven methodology to help with prioritization. The key is to determine three things about each system that's a candidate for protection: Vulnerability, likelihood and impact. In other words, looking at how vulnerable a component is to attack, how likely it is that an adversary will conduct an attack, and how much harm would result from a successful attack. A particular weapons system might have a gaping vulnerability. But there may also be little chance an adversary will focus on exploiting that hole. Or it may be that an attack on that vulnerability wouldn't cause a big problem in the weapon's functioning. In either of those cases, there's no reason to make hardening it a high priority.

Similarly, protecting weapons that rate high on all three vulnerability elements, likelihood, and impact has to be a top priority. Once the top priority components are protected, the government can use the methodology to continue down the list of priorities to guard as much of it as resources allow.

Legacy weapons systems, or at least the processing components of those systems, will gradually be replaced with up-to-date, higher-tech versions. When that happens, designs can integrate cyber hardening into these new systems and components' initial development process. Bolting on cyber hardening afterward, or even introducing it late in the development process, won't be enough to protect against the growing range of new vulnerabilities in our increasingly complex systems. For example, artificial intelligence (AI) will inevitably become an integral part of weapons systems. Protecting AI-based components against future threats is the sort of hardening that must be "baked in" to a system during development, not added on further down the road when the threat fully materializes.

These new, better-protected systems have to be resilient. Successful cyberattacks are becoming more frequent, and no component is immune. That's why the future's hardened systems will incorporate parallel hardware and code that perform the same functions in different ways. If a successful attack impairs some function in the system, the parallel components can detect the problem and take over, restoring the function. Simple redundancy isn't good enough; an attack that takes down a component will probably take down any version in exactly the same way. For resilience, these parallel versions have to rely on different designs.

Cyber hardening used to be a distant afterthought in weapons design. Now it's becoming a prime consideration. Today's techniques will still need to evolve to keep up with emerging threats, but at least the required hardware and software will be in place inside the heart of the system so that they can be updated. That's a significant improvement over having to bolt protections on, and one that will make our weapon systems safer for decades to come.

ABOUT LEIDOS

Leidos is a Fortune 500® information technology, engineering, and science solutions and services leader working to solve the world's toughest challenges in the defense, intelligence, homeland security, civil, and health markets. The company's 38,000 employees support vital missions for government and commercial customers. Headquartered in Reston, Virginia, Leidos reported annual revenues of approximately $11.09 billion for the fiscal year ended January 3, 2020.

leidos.com

LINKEDIN: LEIDOS **FACEBOOK: LEIDOSINC** **YOUTUBE: LEIDOSINC** **TWITTER: @LEIDOSINC**

leidos