Northrop Grumman Whitepaper

Speed Wins: The Next Strategic Technology Advancement for Continued US Military Dominance

Author:

Vern Boyle
Director of Technology, Cyber Division
Advanced Cyber Technology Center
June 2015

Northrop Grumman Corporation
Information Systems Sector
7575 Colshire Drive
McLean, VA 22102

703.556.1000
www.northropgrumman.com
Email: ACTC@ngc.com

~The Relevance of Non-Kinetic Technologies~

The United States has enjoyed a position of military dominance for decades. This dominant position has deterred nuclear threats, defeated terrorists, and protected the homeland with a breadth and depth of advanced war fighting technology. Two of the more significant technological advances have been the development and deployment of stealth, and the use of precision guided weapons. While there are many technologies within our military arsenal, these two examples are arguably ones that shifted the advantage to an extent that was in many ways insurmountable by most adversaries. These strategic technologies were driven by the fundamental goal of fighting and winning on a kinetic battlefield.

In the future, it is conceivable that a widespread cyber-attack could simultaneously strike a combination of civilian critical infrastructure and allied military targets on a scale that would make it impractical to determine the source of the attack, much less determine an appropriate response. This next generation of conflict will be won or lost on a digital battlefield, possibly before the first shot is ever fired. Kinetic technology and weaponry will have a limited role in this type of fight. In fact, some of these weapon systems could be rendered useless by disabling the information or compute platforms on which they have come to rely. Paralyzing a multibillion dollar warfighting machine with computers is a very realistic scenario. The next strategic technology for continued US military dominance will be driven by the fundamental goal of fighting and winning on a non-kinetic battlefield. This strategic technology advancement will need to be addressed with the same level of commitment as a stealth or precision guided weapons program.

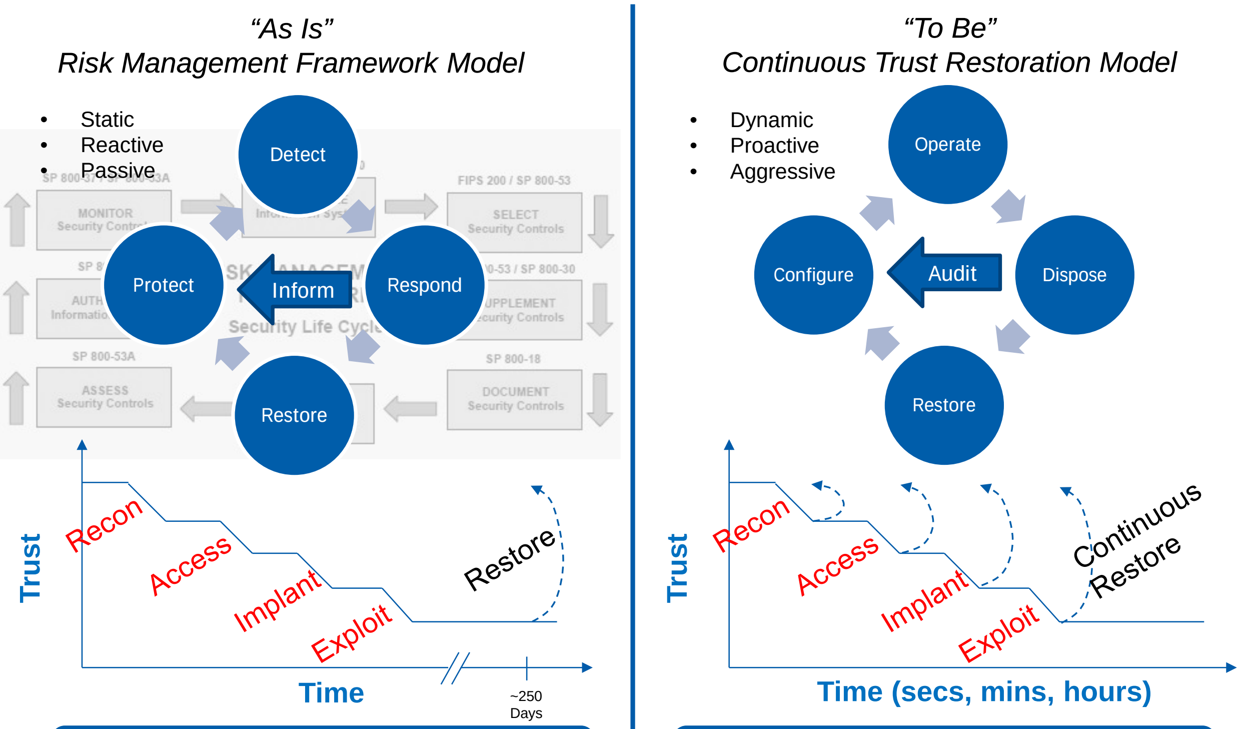
~Speed is the Key to Achieving Strategic Advantage in Cyberspace~

Each week, the report of another high profile breach supports the assertion that we are currently losing the battle in cyberspace. Millions of people are affected, and millions of dollars are lost each year. There are also many examples of breached military and critical infrastructure systems including cases of destructive malware. Why does the advantage seem to be so heavily skewed in favor of the attacker? Why does it seem like our current protection strategies are so ineffective? Simply put, the attackers have fully automated their capability which allows them to gain a temporal advantage. A cursory review of a few statistics shows that millions of new malware samples are generated every year and the breach rate is increasing by double digit percentages each year. These statistics are a result of machine driven operations. People aren’t generating the malware. It is common for an attacker to provision points of presence and command and control nodes that exist for mere minutes. Once again, this is a machine driven operation. This is a highly dynamic automated system with an agile command and control construct. Attackers exploit inherently vulnerable commercial software and hardware to facilitate their operations. These are the adversaries underlying enablers on the digital battlefield scenario painted above.

Contrast this picture with the current state of practice for protecting systems. Network infrastructure is largely static or rarely changes, providing a fixed target. Defense in depth monitoring systems across the network are also fixed, and rely heavily on prior knowledge of an attack to be effective. Both the network and security tools are configured and controlled by people. The people are trained to comply with standards that reinforce the legacy model of fixed, risk management framework based configurations. Weapon systems, platforms and critical infrastructure are assumed to be protected inside untouchable enclaves that are built using this same strategy. The interoperability goals of network centric systems, and the future internet of things, which is expected to reach over 20 billion interconnected devices by 2020, exacerbate these issues. So we have a highly automated machine driven system attacking a static human driven system. The attackers have essentially achieved a currently insurmountable strategic advantage as a result of speed. A protection strategy based on speed, and leveraging a similar dynamic architecture, can shift the advantage toward the defender and defeat many automated attack processes. Modern tools can be applied in new ways such that defenders can negate the temporal advantage of the attacker. A protection strategy based on speed can potentially overcome some of the inherent vulnerabilities in the commercial software and hardware, as well as potentially defeating insider threats and supply chain threats.

~ Continuous Trust Restoration: A Revolutionary Protection Strategy~

Static human driven protection strategies evolved from the underlying network and compute platforms of the past. Over the last 5-10 years, new software defined building blocks have emerged, and new agile/mobile computing platforms have emerged. Software defined networking, network function virtualization, cloud and mobile computing with micro-virtualization are the new tools of the trade. These new technologies create the opportunity to revisit how infrastructures are built and controlled. They create the opportunity to revisit standards and processes such that they can be faster, automated and more dynamic. Rather than fixed systems monitored by people, we have the opportunity to build logically disposable systems that can rapidly change over time. Continuous Trust Restoration is a new concept designed to proactively disrupt an attacker’s kill chain. Rather than detecting and responding using antiquated, slow and often ineffective methods, defenders can restore systems to a known trust level on a continual basis. In its fully realized form, this method would reduce an attacker’s dwell time by orders of magnitude, and limit their ability to access and exploit mission critical systems. Automating the continuous trust restoration process shifts the temporal advantage to the defender.



Highly Automated Adversary Dwells Unfettered on Target for Many Months

Highly Automated Restoration Techniques Continuously Break Kill Chain

Popular equipment vendors are demonstrating early continuous trust restoration concepts with new technology that can achieve the speed needed to shift the strategic advantage away from the attacker. Many of these concepts can extend beyond the network and into weapon systems, platforms and critical infrastructure. This new model is radically different and perhaps disruptive from a current CONOPs perspective. However, it is achievable now from a technology perspective.

~The Rise of a New Non-Kinetic Strategic Technology~

In the future, deterrence, military power projection, and homeland security will depend on a defensible and resilient cyber infrastructure that can operate through widespread cyber-attack. This defensible and resilient cyber infrastructure will be as strategically important during large scale conflict as stealth or precision guided weapons. Speed is the key attribute of this new strategic technology, and is critical to shifting the advantage away from the attacker. There are many emerging technical building blocks that can be used to build this new defensible infrastructure. The time is now to initiate the rise of a new non-kinetic strategic technology that can ensure continued US military dominance.