Federated Cybersecurity Policy Arbitration

Gregory Wehner, James Rowell, Joseph Langley, Joseph Mathews

US Naval Research Laboratory
Center for High Assurance Computer Systems
4555 Overlook Ave SW
Washington, DC 20375
Phone: 202.404.0592 Fax: 202.404.7942
gregory.wehner@nrl.navy.mil, james.rowell@nrl.navy.mil,
joseph.langley@nrl.navy.mil, joseph.mathews@nrl.navy.mil

***Abstract* - Federation promotes a strong cybersecurity posture for inherently decentralized networks. Dictating cybersecurity policy through traditional top-down approaches has engendered stagnation in network defense as cybersecurity personnel become preoccupied with compliance rather than the intent of the policy. Permitting variations of policy among network enclaves protects local mission function and increases the potential for innovation across the organization when integrated into cybersecurity baselines. Federation gives network enclaves the freedom to exercise their authority to respond to local threats and promotes ownership of their network, without diminishing the benefits of cybersecurity baselines. This federated model paves the way for an automated defense matrix in which independent, autonomous agents evaluate network data to create actionable cybersecurity policy to be shared, modified, and deployed among a web of other agents in near real time. Federated security policies promote a resilient posture through heterogeneous defense in breadth, while creating an internal mechanism for continuous adaptation and innovation in security approaches. Federation should be a core design tenet for cybersecurity technology.**

I. INTRODUCTION

Networks are not under attack; they are under siege. Industry trends towards orchestration and automation challenge large organizations that are effectively a patchwork of diffuse networks. For such organizations, strategies that rely on unified enterprise solutions run the risks of micromanaging network enclaves and creating a weak homogeneous cybersecurity posture [1]. At the same time, such strategies are critical to securing the network by providing baseline policies: rules for network access, secure configuration guidance, common defense architecture, acceptable software and hardware offerings, and continuous updates to known vulnerabilities. The practical expression of this tension occurs when global security policy degrades local mission function or when a global policy fails to address a discrete localized risk. A federated approach to network defense resolves these conflicts.

II. FEDERATION

Recently, Federation has been regarded as the notion of creating interoperability between disparate information systems [2], [3]. With respect to cybersecurity, we expand upon this notion to define Federation as a method to arbitrate among independent enclaves of a distributed network.

In enterprise technologies evolved from manager/sensor architectures, policy is created at the top of the organization and subordinate enclaves are limited to redistribution and consumption. If a conflict occurs between a policy and subordinate mission function, a network enclave has few options. The enclave can isolate themselves from the policy creators or apply the policy and accept the degraded function until the policy or the mission is altered.

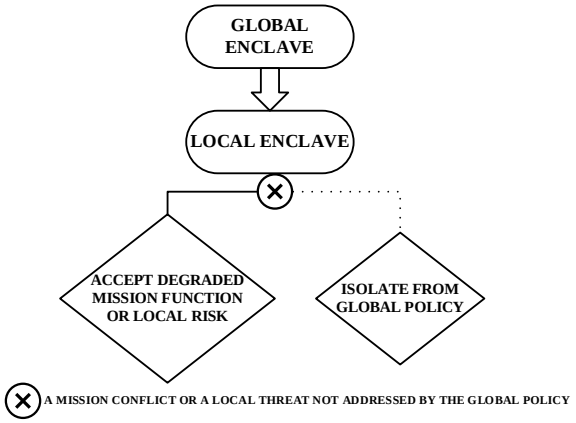

Figure 1: Policy flow in traditional network defense paradigm limits enclaves.

Federation supports the authority of the enclave. When a conflict with a policy within a cybersecurity baseline occurs, a federated enclave can discretely reject the policy, modify the policy, or accept the policy.

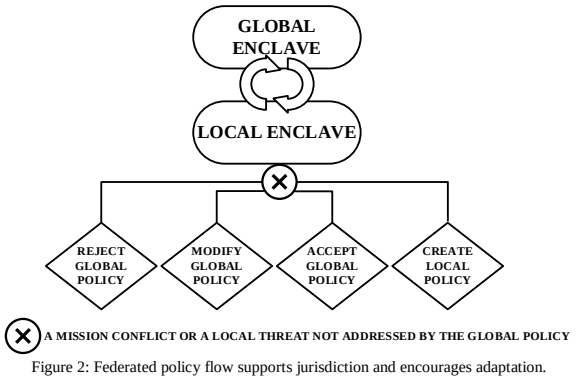

Figure 2: Federated policy flow supports jurisdiction and encourages adaptation.

The enclave may also create new policy to address local risks not covered by the baseline. This shift returns focus to local ownership, without diminishing the relevance of cybersecurity baselines.

III. ADAPTATION

Cybersecurity personnel at network enclaves spend time and effort implementing cybersecurity baseline requirements (i.e. checking boxes). However, local attributes such as mission, location, personnel, asset value, and external partnerships are all unique factors that contribute to risk at an enclave. These factors change frequently, making it difficult for an organization to address every risk with a cybersecurity baseline. Yet rather than creating policy aligned to the risk profile at their enclave, cybersecurity personnel are preoccupied with administrative tasks. This has promoted stagnation, with cybersecurity personnel disengaged from active defense.

Federation resolves stagnation through promotion of innovation and adaptation. When a network enclave encounters a mission conflict or a localized risk, Federation supports the enclave's authority to modify or create new policy. Given the breadth of talent within the enclaves, it is likely that a solution to a local conflict will provide benefits throughout the organization. While not all adaptations will be relevant beyond the local enclave, analysis of this feedback provides a heterogeneous source of innovation that engages cybersecurity personnel in defending their enclaves and fosters resilience throughout the organization.

IV. JURISDICTION

Federation enables network enclaves to defend themselves according to their authority. This extension of responsibility to the enclave reinforces accountability amongst cybersecurity personnel as attributable successes and failures invests all in creating a strong defensive posture. Federation does not infringe on the benefits of cybersecurity baselines. Enclaves without the resources to tailor baseline policy to their unique risk profile would simply implement it as-is.

Federation is not a call for anarchy, nor are we advocating that each operator or enclave have blanket authority to change or reject policy. Federation does not grant authority. Organizations under Federation will continue to structure their networks as strictly or loosely as their guiding bodies determine. For example, a federated network may behave similar to a judicial appeals process; challenges to global law are heard by local authorities, work their way up to regional bodies, and eventually may be integrated as global amendments.

V. CHALLENGES

Our assertions about Federation are open to several relevant concerns. Solutions such as security as a service (SECaaS) and deployment in the Cloud may reduce security cost, defer risk, and blur the boundaries of network enclaves, calling into question the utility of Federation. In rebuttal, making the boundaries invisible to the client does not remove them. Risk deferred is still risk, and a federated approach applies to Cloud and SECaaS providers alike. Wherever an organization has internal policy conflicts, Federation will be a viable strategy.

Extending more responsibility to local enclaves requires resources for training and specialized talent, outside of those required to create cybersecurity baselines. An untrained cyber workforce at one network enclave threatens the security of the whole network. Yet, with billions spent annually on cyber defense [4], cybersecurity incidents continue to rise at an alarming rate [5], [6]. The current approach to cybersecurity has become stagnant, and without a shift, the return on investment on cybersecurity will diminish.

Adaptations are only relevant if they are vetted, presenting a strain on the global creators and potentially introducing as many failures as successes – if they are implemented at all. While this culture shift will doubtless come with a learning curve, sourcing innovation from all levels of an organization has proven successful at technology companies such as Google [7] and Amazon [8]. As the Federation is refined at an organization, best practices will emerge to optimize the method and format of communicating policy, streamlining the vetting process and shortening the time to distribute new ideas.

A federated organization is harder to direct from a central governing body, as each enclave exercises their independent authority. A homogenous network is simpler to manage than one where each enclave has a unique defense policy. To the former, the organization determines how much authority the federated enclaves have. However, if an enclave has authority, they should be trusted to exercise it. To the latter, being simpler to manage does not translate into being simpler to secure. "Just like genetic diversity, which prevents an epidemic from wiping out a whole species at once, diversity in software is a good thing." [9]

VI. LOOKING AHEAD

The cybersecurity marketspace is becoming increasingly automated [10], with artificial intelligence and machine learning techniques being introduced into anomaly detection and predictive analytic applications across the spectrum of cybersecurity solutions. Future autonomous agents will analyze data from throughout the enclave: network traffic, vulnerability scans, log files, behavior models, etc. Agents will search the data for indicators of attacks and weaknesses in the enclave's cyber defense posture. As the agents become trusted in identifying attack vectors, they will be deployed to author cybersecurity policy to quickly pivot resources and strengthen the cyber defense posture. Such policy will be an invaluable source of threat intelligence and shared with designated enclaves throughout the organization. These enclaves will correlate the intelligence with their own data – weighted on factors such as proximity, network similarity, organizational relation, and source authority. This will form a resilient, symbiotic defense matrix.

Federation paves the way for these defense matrices to share policy with the organization. As autonomous cybersecurity solutions become more prevalent, the concerns about Federation will become less relevant and the benefits more apparent. In order to promote persistent resilience in network defense and to prepare for the reality of autonomous cybersecurity, Federation must become a core design tenant in cybersecurity technologies and organizational structures going forward.

VII. REFERENCES

[1] J. Cobb, "Centralized Execution, Decentralized Chaos: How the Air Force IS Poised to Lose a Cyber War," *Air & Space Power Journal*, Summer 2011, pp. 81-86

[2] N. Suri et al., "A Dynamic and Policy-Controlled Approach to Federating Information Systems," *Proc. 2010 Military Communciations Conference* (MILCOM 2010), 2010, DOI: 10.1109/MILCOM.2010.5680377

[3] M. Brannsten et al, "Toward Federated Mission Networking in the Tactical Domain," *IEEE Communications Magazine*, vol. 53, no. 10, 2015, pp. 52-58

[4] Gartner, Inc., "Gartner Says Worldwide Information Security Spending Will Grow 7.9 Percent to Reach $81.6 Billion in 2016," Aug. 2016; www.gartner.com/newsroom/id/3404817

[5] "Federal Information Security: Actions Needed to Address Challenges," US Government Accountability Office report GAO-16-885T, 19 Sept 2016.

[6] *Verizon 2016 Data Breach Investigations Report*, tech. report, Verizon, 2016.

[7] A. Steiber and S. Alänge, "A corporate system for continuous innovation: the case of Google, Inc.," *European Journal of Innovation Management*, vol. 16, no. 2, 2013, pp 243-264

[8] J. Dyer and H. Gregersen, "The Secret To Unleashing Genius," *Forbes*, Sept 2nd, 2013.

[9] C. Stoll, *The Cuckoo's Egg: Tracking a Spy Through the Maze of Computer Espionage*, Pocket Books, 1990, p. 58

[10] *State of Security Operations: 2016 report of capabilities and maturity of cyber defense organizations*, business white paper, Hewlett Packard Enterprise, 2016.

[11] E. Rzeszutko and W. Mazurczyk, "Insights from Nature for Cybersecurity," *Health Security*, vol. 13(2), 2015, pp. 82-87.

[12] "The DoD Cyber Strategy," US Department of Defense, April 2015.

[13] P. Small, *Defense in Depth: An Impractical Strategy for a Cyber World*, CreateSpace Independent Publishing Platform, 2011.