The Nihilistic Network Management Model (N2M2): An Optimal Approach to Cybersecurity

Dr. Edgart Notting[1], and Anonymous[2]

[1] Department of Metaphysical Informations Technology, Cranberry-Lemon University, Pittsburgh, PA, USA
[2] Foundation for Anarchist Computer Science, Cranberry-Lemon University, Pittsburgh, PA, USA

Abstract

In Network Management, the administrator must balance performance, convenience, flexibility and security to provide a reliable service to their client applications. The classical and enlightenment era network management models have been shown time and time again to fall prey to fast developing and adaptive malware. Before malware was advanced, such classical methods provided an effective simplistic approach to maintaining the performance benchmarks that network clients have grown to expect. Unfortunately, under the complex cyber security environment, only extremely rigid religious fundamentalist network management methods remain secure at the price of strict configuration management and slower performance. Using a new Nihilistic Network Management Model (N2M2), extreme metaphysical and epistemological skepticism are utilized to create secure networks while keeping configuration management flexible and expedite network performance to evolve into an übernetwork. The N2M2 is shown in this paper to be 98% more likely to prevent a phishing attempt while maintaining performance benchmarks with extremely flexible network policies.

1. Introduction

In the modern world, any network is just a few bad clicks away from DDoS attacks, ransomware, and costly leaks of sensitive information. With cyber security illiterate boomers taking longer and longer to leave the workforce, those bad clicks and phishing email replies aren't going away any time soon; meanwhile, cyber threats are only growing.

As all network management techniques go, most administrators follow a particular philosophy based model [1]. Data agnostic methods may have been effective in the past but the increasingly complicated security environment has made it impossible. You could use the *Firewall and Brimstone* approach for the most secure method but suffer in performance and an extremely strict configuration management. Even classical methods are not ideal; as Stoic methods are prone to ignoring worldly problems and the Platonic method can never settle on the ideal form of the server.

It turns out that the ideal network management model should be based on a 19th century nihilistic philosophy. Not only is the configuration management flexible, but the anarchist deconstruction of faults will improve performance. It is nearly perfect for cyber security practices as malware cannot have a significant effect on a network's client applications if that network proves to the client and user level that the malware is devoid of all meaning.

2. Background

In network management, the administration has to balance and fulfill five major goals. Fault Management, Configuration Management, General Administration, Performance Management, and Security Management. In fault management, the administrator tracks and fixes faults in the network. In configuration management, protocols, devices, firmwares and such are standardized. Administration work consists of managing user passwords, permissions and a general client interface. Performance management is the process of benchmarking and improving the performance of the network to avoid stagnation and continually optimize network resources. Finally, security management prevents malware from infecting clients by means of firewalls, proxy servers, anti-virus software and general network policy.

The N2M2 method is the antithesis of traditional philosophical network schools of thought. It has a highly skeptical framework which is perfect for cyber security applications. Applying cosmological, epistemological, political, and metaphysical nihilism to the network

management process, most configurations and practices are deconstructed to a point that is unrecognized by malware. The old ways may have worked in the old world of cyber security but nihilistic network managers strive to shed themselves of useless infrastructure which turns out to be meaningless and only look forward to creating an übernetwork.

3. Comparative systems

Before understanding the N2M2, the traditional approaches must be deconstructed. Most network management philosophy is covered by Agnostic, Platonic, Stoic and Religious Fundamentalist categories. These thought process heuristics were developed in the early days of the internet. To understand the direction of the N2M2 it is important to understand what values it will be deconstructing.

3.1 Agnostic Methods

In a perfect world, the agnostic method would be ideal. The agnostic network management techniques don't assume anything about the network, the devices, or the data. Whether the data is using a TCP protocol or UDP protocol, or an antiquated device, operating system or firmware, an agnostic method will treat it all the same. This is a great method for P2P type networks and general flexibility; however, such Laissez-Faire methods can end up inefficient and prone to vulnerabilities.

3.2 Platonic Methods

Network Management through Platonism revolves around implementing ideally formed proxy servers, switches, and firewalls and is best expressed through this excerpt from one such defining dialogue in [2].

Socrates: Would you not say that a network is either secure or it is not secure.

Polus: I suppose

Socrates: and would you not also agree that a network manager who allows malicious activity to be a bad network manager.

Polus: This is also true.

Socrates: Then assuming a bad network manager is the opposite of a good network manager, the practice of tracking and preventing malware would make a network secure and a good network manager.

Polus: Obviously.

Socrates: So every act of the good network manager would be to prevent such vulnerabilities?

Gorgias: Socrates, that is a misleading question, there are too many other functions of the Network Manager to be distilled into one form! Your rhetoric is terrible.

Several pages and dozens of questions later in [2], a platonic ideal of a network management scheme is achieved and found to be sufficient.

Unfortunately, in practice the Socratic line of questioning often views small problems as a sign that the management method is not perfect and many working systems are scrapped at the first fault or data leak even if a small patch is required.

3.3 Stoic Methods

The Platonic network management model eventually evolved into a virtue ethics based Stoic model based on [3]. In this method, the functions of network management are thought as ultimate virtues to live by. Unlike the Platonic ideals, the stoic method understands that one vulnerability does not mean an entire network is bad.

"Network management does not promise to secure anything from an external system, otherwise it would be admitting something that lies beyond its proper Domain's Local or Wide Area Network. For as the material of the carpenter is wood, and that of statuary bronze, so the domain of the art of network management is each administrator's own." Epictetus [3].

While the focus on virtues improved the endurance over stoic methods beyond the short lived Platonic models, such thinking produced dismal fault management. When the stoic managers understood that network faults and security holes may be out of their own locus of control, there was no incentive to adjust the network virtues to the changing but flawed world of cyber security.

3.4 Religious Fundamentalist Methods

Once the network management community determined that the classical and enlightenment heuristics could not holistically maintain benchmark performance while remaining secure in an ever growing sinful world, many turned to the 19th century great awakening for inspiration. As famously coined the *Firewall and Brimstone* approach, the methods based on religious fundamentalism have been shown to be the most secure to date [4].

These methods are the bread and butter of strict bureaucratic organizations due to massive network size or slow government policy in a state application who don't have the resources to hire Stoic-Platonic network managers. These organizations can't risk data spills so they don't risk anything by sending all the good data to the cloud and all of the bad data to a stand alone data server in the basement to likely never see the light of day again before filing a report months later.

The *Firewall and Brimstone* approach unfortunately attracts the most criticism from clients. Determining which data gets to go to the cloud is determined through extremely

strict configuration management across applications and protocols, as well as harshly judgemental firewalls. Many systems using this method only have the resources to manage on one type of OS and and sometimes even one web browser, severely limiting the freedom of the client.

Additionally, many of the religious methods are rarely developed centrally which makes them slow to adapt to faster changing cyber security environments. This is the result of major divides when *Firewall and Brimstone* methods became first popularized. Most of the major telecommunication networks could not uniformly decide on what methods or *required sacraments* would constitute a secure protocol. While they may look the exact same on the outside, these networks are fundamentally different and incompatible with each other unless branching from the same network denomination. [5]

3. The Nihilistic Network Management Model (N2M2) Architecture

The N2M2 model attempts to bridge the world of agnostic configuration freedom with the security of a religious system. Many of the methods are only possible by the Nihilistic manager's belief that a network cloud does not actually exist. With such traditions deconstructed the network management can be modeled as Figure 1 below.

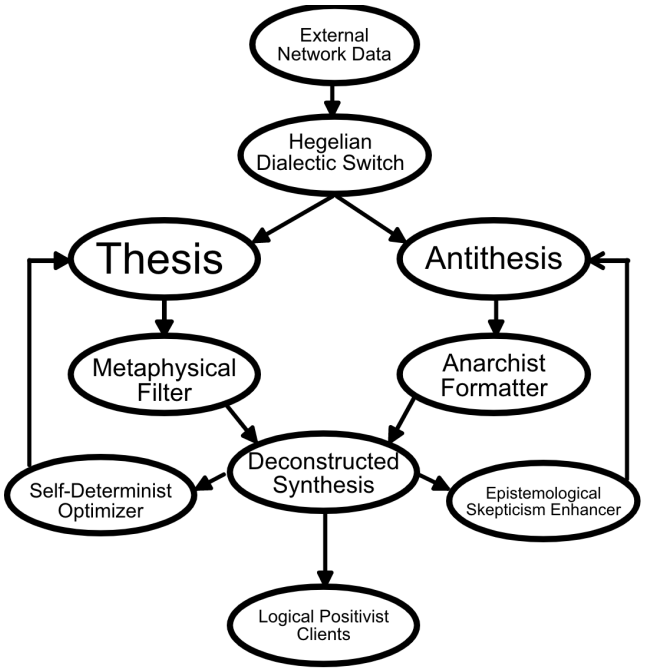

Figure 1: N2M2 architecture

As in most pre Karl Popper network models, the external data is first passed through the Hegelian Dialectic Switch [6] where each data packet is posed as good in the thesis javascript node and misformatted or malicious in the Antithesis node. The thesis proposition then has any metaphysical notions about it's nature or meaning in the world's Wide Area Network (WAN) filtered out. Similarly, the antithesis proposition amplifies edgy new non-malicious formats that are being held back by Interface Control Documents (ICDs). In order to rage against the ICD, that data is still weighed in at the synthesis node.

At the synthesis node, the filtered content of the data packets are routed to the materialistic Logical Positivist Clients who are happy to get their data whether it is enlightened against a conservative aesthetic or not. At that point, only logically consistent data with displayed uncertainty exists and no harm can be done because the data now has zero meaning attributed to each packet.

Results in the synthesis node are then fed backwards to the dialectic node handlers using the self-determinist optimizer and the Epistemological skepticism enhancer. These two nodes allow the N2M2 to improve over time by encouraging the thesis to consider a wider range of data structures and devices while increasing the epistemological skepticism to continually improve cyber security. To convey the lack of meaning to the client a Shaupenhauer skepticism tag was applied to data that got to the application layer.

4. Test Methodology

This architecture was prototyped using Javascript Nodes. Because each node did not agree with each other in any operating system, or written in the same JS library or environments, they had to all be separately containerized. Then the interface between each node was put into its own docker container. With all of the interactions in a stable container image, they were then built into an overall container image which could be implemented on real hardware. With only three layers of docker containers the N2M2 was finally able to be tested.

Red-Blue team testing was applied in a simulated network to determine how effective the N2M2 would be at identifying faults and vulnerabilities while maintaining and improving network performance. Though it was only a simulation, the results are likely to be accurate because three of the nodes have already determined that we are probably living in a simulation anyway in the process of testing.

5. Results

The N2M2 performed as expected. Very few malicious content survived the dialectic switch. The majority of those problems only occured before the system learned to question everything that was routed through Russian servers or had spam words such as Viagra and penile enlargement. Overall, the performance only increased once new nihilistic metrics were established.

5.1 Performance

At first the N2M2 had a lot of downtime and dropped most of the packets. Many of the packets were getting filtered out by the metaphysical filter for containing uncertain knowledge derived from structurist Judeo-Christian propaganda. The Russian Nihilist anarchist node even began labeling most of the data as Tsarist Totalitarianist ideology.

Giving the data a second look, we normalized the data to look publishable like any good researcher. The normalization was based on the feedback produced by the optimization node framework to determine what true non-propaganda data was getting through to the client. That is when it appeared to be working perfectly. As shown in figure 2, the system was not dropping any data after running the N2M2 for a few hours despite what our materialist clients were complaining about.

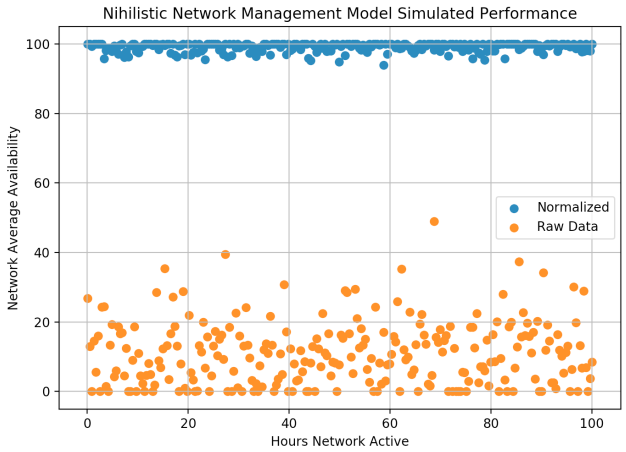

Figure 2: N2M2 Network Availability

5.2 Configuration

Throughout the entire test, the system was able to connect different users using any type of operating system or protocol. It was even able to support deprecated browsers, functions and data types. With flash finally securely supported by the N2M2, it is only through Nihilism that you can watch Homestar runner the way it was meant to be viewed without risking a virus.

5.3 Security

Even before the epistemological skepticism node optimized the dialectic splitter, not one email or data packet got through without being flagged as a dangerous proposition that there is meaning in this email when there is zero evidence that such meaning could be derived from something as simple as a cat meme or a two hour scheduling meeting from Linda.

While maintaining the normal level of security filtering as a typical firewall, users were even less likely to fall prey to phishing attempts. By the time users finished reading the warnings from Schopenhouer's Western Buddhist nihilism to give up all desires in order to reduce suffering, the materialistic clients were shown to be 98% less likely to click on scam emails which preyed on such vulnerabilities from human desire. There was no point in extending a car warranty when it was clear that it would not bring metaphysical happiness or reduce suffering in any way.

6. Conclusion

Shown by these results, it is obvious that the N2M2 is the network management model of the future. There is finally proof that nihilism is useful for something despite not even being an ethos such as national socialism. The important question now is where to go with this new revolutionary approach to network administration.

In early propositions of a nihilistic approach to network management, [7] proposed that there would be two paths, active and passive. A passive N2M2 would be primarily self contained such as the centralized religious networking models. On the other hand, in an active N2M2 approach, the Schopenhauer metaphysical spam warnings could spread outside of the N2M2 area networks and reach the world. In this frame, the nihilistic method's ultimate goal would be to make the entire internet use the N2M2 framework. According to [7], if the entire world is using a nihilistic framework to manage their networks, there wouldn't even be a need for network managers in the first place. This is what is called the übernetwork.

Until the utopian meaningless network exists where the device layer directly connects to the application layer, the need for secure networks will remain and the N2M2 is now shown to be the only model which perfectly balances the needs of even the most materialistic, intellectually traditional client applications with the security of a world designed to exploit man's inner desires and weaknesses.

References

[1] Kant I. 1792 *The Necessity of Metaphysical Frameworks in Modern Network Theory :: Journal of Enlightened Network Managers*

[2] Aristocles Approximately 362 BC *The Ideal Forms for a Secure Network Against Rapidly Developing Cyber Threats :: Dialogues from an Archaeological Dig in Athens*

[3] Epictetus. Approximately 128 AD *Virtue Ethics Discussions in Information Technology :: Dialogues from an Archaeological Dig in Turkey*

[4] Smith J. 1842 *The Book of Cyber Professionals of Latter Day Saints Chapter 8*

[5] Brother Thelonious. 1952 *A Comparative Study of Denominational Network Management :: Vatican Seminary for Wayward Protocols*

[6] Popper K. 1943 *A Critique of Dialectic Based Network Techniques :: Journal of Post-Modern Computer Science*

[7] Nietzsche F. 1884 *The Ubernetwork and Man's Evolution towards Cyber Security Utopia:: Journal of Mistranslated Philosophical Works*