Network Access Control (NAC): An Open Source Analysis of Architectures and Requirements

Gloria J. Serrao
Senior Technical Development Program
National Security Agency (NSA)
9800 Savage Road
Ft. Meade, MD 20755

Stevens Institute of Technology, Systems Engineering
Masters' Degree Project

Abstract: The main goal of NAC is to extend the security of networks to the end-point by measuring the authenticity, integrity and security posture of each end-point prior to granting network access. To do this, the following functional areas must be present: authentication/authorization, assessment of security posture, quarantine and remediation. This paper presents an overview of an in-depth NAC requirement analysis performed against three NAC products based entirely on open source literature. The emphasis of the analysis was to define functional and security gaps across all products and make recommendations to improve the overall security and interoperability of NAC products.

This paper identifies:

- Key design and implementation choices that are required based on stakeholder requirements
- Areas where NAC does not meet stakeholder(s) requirements
- Areas that have not been adequately defined for implementation
- Recommendations to improve the security posture of NAC products.

An analysis of each product is performed in the following areas:

- System Administrator Interface and Policy Settings
- Authentication
- Integrity Measures
- Remediation
- Security
- Functional
- Non-Functional

This analysis and research of NAC lead to seven general recommendations for improving the security of NAC products and four recommendations for deploying and implementing them.

Index Terms – Network Access Control, Integrity, Authentication, Trusted Computing Group (TCG), Trusted Network Connect (TNC)

1. Introduction

Endpoint security is taking on a larger role in overall enterprise security planning. Authentication and integrity of the endpoint are equally important for a NAC solution. Integrity is the purity of an endpoint from harmful hardware and software. This paper will discuss architectures being developed for NAC and analyze NAC requirements (derived from the architectures and open literature) against three products. Recommendations are then made for viable and secure implementation.

The Trusted Computing Group has defined the architecture for NAC as well as a framework for interoperability among vendors. It has published an extensive set of architecture descriptions including the TNC Architecture for Interoperability specification [1] that describes the components required for a NAC solution and how they should communicate. In addition, the TCG has developed eight separate architecture documents that describe the internal interfaces between each component. The TCG TNC architecture description was used to gather and refine NAC requirements for this paper. A draft IETF standard for Network Endpoint Assessment (NEA) was also used as a requirement source. [2] In April 2010, this draft was approved and became two IETF standards entitled "PA-TNC: A Posture Attribute (PA) Protocol Compatible with Trusted Network Connect (TNC)"[3] and "PB-TNC: A Posture Broker (PB) Protocol Compatible with Trusted Network Connect (TNC.)"[4] These standards are compatible with the TCB TNC specifications.

Customers for NAC solutions include: financial and educational institutions, businesses, health care providers, and government. Within each of these there are the following types of stakeholders: system administrators, information technology specialists, network users, data owners, and corporate executive officers. Major drivers for the use of NAC are the Health Insurance Portability and Accountability Act (HIPAA) and the Sarbanes-Oxley Act of 2002 that address federally required protections for personal health information, public company accounting reform and investment protection.

This paper analyzes NAC requirements from the perspective of stakeholders, but emphasizes security requirements. It also reviews non-functional requirements such as performance and usability.

2. NAC Basics

NAC provides endpoint management and compliance, identity management and company/agency usage policy enforcement. This paper will reference NAC components as endpoint, verifier and enforcement point or enforcer. Each vendor has its own unique naming scheme. The recently approved IETF standards for NAC reference the components as collector and validator (of posture attributes), broker (distributes attributes) and transport (responsible for secure transport):

978-1-4244-7402-8/10/$26.00 ©2010 IEEE

Client Components:
- Posture Collector
- Posture Broker Client
- Posture Transport Client

Server Components:
- Posture Validator
- Posture Broker Server
- Posture Transport Server

The three entities described in this paper: an endpoint, a verifier and an enforcer are also referenced as the endpoint, policy decision point (PDP), and policy enforcement point (PEP), respectively. The enforcer is most often the network switch or hub, firewall or VPN gateway that enforces the access decision made by the verifier.

Each of the major NAC components has multiple levels of communication protocols for exchanging authentication and integrity information. The TNC recommends interoperable protocols at the different layers of the International Standards Organization (ISO) network protocol stack.

The heart of the NAC solution lies in the assessment logic of the verifier and how the verifier determines that an endpoint is "pure" or "good." The decision is then communicated via a defined protocol from the application layer to the network layer and is passed back to the enforcer at the network perimeter that denies or allows access to the network at a layer 2 or 3 device. Allowing the system administrator easy but granular policy settings and views into the decision logic is important for user acceptance of a NAC solution.

Figure 1 demonstrates that NAC functionality is often achieved by creating sub-enclaves, each with a specific purpose. One is the secure network, one is where problem clients are repaired and a third (the entry point) can be considered an enclave where the authentication and integrity assessments take place.

3. Basic Communication Flows in a NAC Product

The NAC communication begins when an endpoint authenticates and provides any trusted platform characteristics to the verifier. Both the person and machine authentication should be checked. Then, integrity measures are taken of the endpoint and these are sent from the endpoint to the verifier.

This is where the proper protocols and message handling techniques are important. There can be several rounds of messages about the hardware, operating system and software application status. Once integrity measures are captured and provided to the verifier, it determines if security policies are met. For example, are the latest operating system patches applied?

If policies are not met, remediation is needed and the verifier sends instructions to the endpoint on how it should connect for a remediation process. The endpoint follows these instructions to allow either limited network access or to be placed on a separate network so that remediation can occur.

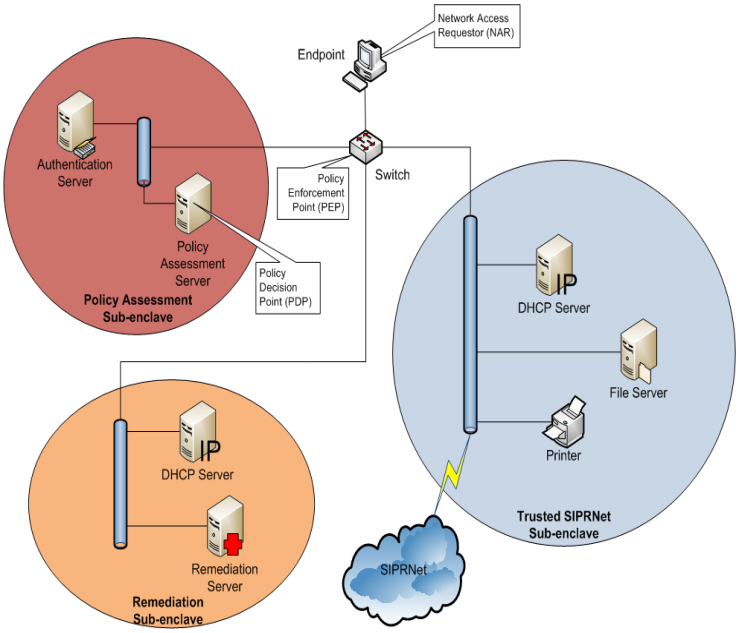

Figure 1 – Sub-Enclaves used in NAC Solutions (Source: IA Component of the Global Information Grid (GIG) Integrated Architecture System Plan, Network Access Control on SIPRnet, Version 1, 20 November 2007)

In addition, after an endpoint is checked for integrity measures, the network administrator may need to apply policies to the endpoint prior to its acceptance on the network. For example, the endpoint may be placed into a virtual private network or other decisions about future access may be determined based on the user role or group it gets assigned at this point.

Not often shown in architecture diagrams of NAC is a separate network for remediation and isolation. It protects the network from the infected client until the client is brought up to the required integrity level. It is important to have this separate network secured well so that there is not a time window where clients with bad integrity are allowed access to the network.

The TNC architecture emphasizes security and allows for the optional use of trusted computing platforms with trusted platform modules. The Trusted Platform Module (TPM) is a microchip on the motherboard that provides a hardware-protected root-of-trust for device and user identity as well as for the storage of integrity measures about the endpoint.

It securely generates keys with a hardware pseudo-random number generator and contains a keyed Hash Message Authentication Code (HMAC) function using a SHA-1 hash generation function and RSA encryption. The TPM creates and securely stores user and platform identity credentials (keys, passwords and digital certificates) for both users and machines. Each TPM has a root "wrapping" key called the Storage Root Key (SRK) which is stored within the TPM. The private portion of keys created in the TPM is not exposed to other entities (components, software,

processes or persons.) The TPM is also used to measure the hardware and software configuration of the endpoint and compare it to a previously stored "known good measure." This TPM functionality greatly enhances the security of NAC. [5]

4. Requirements

A set of stakeholder requirements were created over a six-month period of time by researching current technology articles and the following specifications and requirements documentation:

- Trusted Network Connect Architecture for Interoperability, Specification Version 1.2
- Request for Comment (RFC) by the Network Working Group of the IETF entitled "Network Endpoint Assessment (NEA): Overview and Requirements."
- Requirements from the Enterprise Solutions Steering Group (ESSG) SIPRnet NAC Technical Advisory Group market Research Capability Report, dated May 12, 2008. (The ESSG was established by the Secretary of Defense in September 2003 to standardize network defense tools, capabilities and practices.)
- Information Assurance (IA) Component of the Global Information Grid (GIG) Integrated Architecture System Plan, Network Access Control on SIPRnet, Version 1, dated 20 November 2007

NAC requirements fall into the following major categories: Administrator Interface, Authentication, Integrity, Security, Functional and Non-Functional. A total of 133 requirements were defined and allocated as follows:

- Administrator Interface (17)
- Authentication (42) designated as Authentication for the endpoint (11) system (16), verifier (11) and enforcement point (4)
- Integrity (26) designated as integrity for the endpoint (3), system (12), verifier (3), enforcement point (4) and remediation function (4)
- Security (18)
- Functional (18)
- Non-Functional (12)

For each category of requirements, a review of open source literature was conducted to determine if individual requirements were addressed. If so, it was further noted if the article stated the requirement was met or not met. If the requirement was not discussed or no indication was made as to whether the product was compliant with the requirement, it was noted as "Unknown."

5. Product Overviews

A general overview of each of the three products is now given to provide information about their functionality and architecture.

5.1 PacketFence – Open Source NAC Solution and Virtual Machine Appliance

PacketFence is a Linux-based open-source product with the goal of making NAC available to average users and networks. There is a version that has a VMware appliance that makes the installation and configuration of the product simple. Although initially, only Address Resolution Protocol (ARP) isolation was supported (April 2007) and scalability was an issue, now Virtual Local Area Network (VLAN) based isolation allows for larger-scale network support.[6] PacketFence maps user identities to machine identities and examines the machine posture and instructs the machine to perform self-remediation.

The product can be configured as either an in-band or out-of-band solution. As it an in-band solution, it sits between the client and server and performs address isolation based on ARP or Dynamic Host Configuration Protocol (DHCP). The out-of-band mode uses SNMP traps to change VLAN membership of specific ports. It will detect a MAC address, and if not registered, PacketFence will move the requesting port to the registration VLAN.

To deploy PacketFence in the out-of-band mode, manageable switches are required and must include a means to change a ports' VLAN remotely. PacketFence expects simple network management protocol (SNMP) traps to be sent to it so that a "deny or allow" decision can be made based on IP address, port number and/or MAC address.

5.2 Cisco Network Admission Control (NAC)

The Cisco NAC "framework" is an architectural solution that involves over 75 of Cisco's security partners that seek to make their products compatible and interoperable. Users, however, must make an investment in the complex integration and testing of multiple software, hardware and services.[7] The customer can be sure that these devices work well together and also that Cisco partners' products are interoperable. Cisco and Microsoft have also published an Interoperability Architecture. However, initially both the Cisco Secure Access Server and the Microsoft Network Policy Server must be deployed. Either company's agent can work.[8]

From a product perspective, Cisco integrated a NAC network module into its Integrated Services Routers. This allows users to update their existing router capabilities to include NAC. There is also a stand-alone NAC solution called the Cisco Clean Access Server or the NAC Appliance. The Policy Decision Point (PDP) function is performed by Cisco's access control server which includes interfaces to support vendor supplied policy servers, authentication servers and audit servers. Cisco owns a big part of the network appliance market and therefore, is often viewed favorably by corporations and users that have Cisco components already in place.

Cisco NAC can be deployed as either an in-band or out-of-band solution. An in-band deployment is always in line with user traffic and an out-of-band deployment means that the Clean Access Server (CAS) is in line only during authentication, integrity assessment and remediation. The out-of-band mode uses the Simple Network Management

Protocol (SNMP) to communicate with supported switches. In-band is best for wireless, remote and branch office applications. The out-of-band is better for larger LAN and WAN deployments where enforcement of the access control happens at the switch.[9]

For transport level security, Cisco uses proprietary Extensible Authentication Protocol (EAP)-Flexible Authentication via Secure Tunneling (FAST). This leverages 802.1 x authentications and can include end-point integrity information in the EAP protocol. Cisco also needed to support legacy customers who do not have 802.1x compatible switches. For that reason, Cisco also supports EAP-over-User Datagram Protocols (UDP). As discussed below in the authentication requirements, UDP does not perform authentication so that another mechanism for authentication must be used.[10]

5.3 Microsoft Network Access Protection (NAP)

Microsoft has incorporated NAC functionality in its Windows desktop and server operating system and combines this with a network policy server (NPS). It is scalable because it allows a large number of endpoints to be supported by few NPSs. Microsoft uses its Active Directory for authentication and the Forefront security application to perform many of the functions that NAC requires. Microsoft does not implement the Trusted Network Connect (TNC) specifications. Instead, the company claims through various white papers that it is interoperable with the TNC because of its statement of health protocol (IF-TNCCS-SOH) which is interoperable with any TNC component (client, verifier or endpoint). IF-TNCCS-SOH is a client server protocol for reporting the health of the client; it complements the TNC-TNCCS (which describes client-server interactions.) Microsoft wrote this protocol and it was added to the TNC specifications list after being introduced at Interop Las Vegas in 2007. It allows customers to use NAP within a TNC supported network and TNC in a Microsoft NAP environment.

NAP enforcement points use NAP policy server generated statements of integrity to enforce network access limitations. NAP uses various enforcement methods including: Internet Protocol Security (IPsec), 802.1X, remote VPN connections, and Dynamic Host Configuration Protocol (DHCP) and NAP with NAC enforcement. IPsec is the strongest as it offers access control on a per-connection basis using the SOH X.509 certificate. Other examples of a NAP enforcement point are a DHCP server or routers that support 802.1 x authentications. The use of a DHCP server and its assignment of an IPV4 IP address is weak because a user that has administrator privilege can over-ride a DCHP address configuration.

A NAP enforcement point can also be a Network Policy Server (NPS) and can act as a NAP health policy server. A health policy server evaluates the health state of NAP clients; determines access allowed or remediation to be performed. Microsoft Certificate Authorities are used to issue “health certificates” for compliant computers. For transport level security, NAP uses HyperText Transfer Protocol (HTTP) over Secure Sockets Layer (SSL) or Protected Extensible Authentication Protocol (PEAP) between clients and servers to protect authentication and health state information. IPsec can also be used with IP addresses or port numbers being used as machine identifiers. IPsec uses the MS X.509 client certificates.[11]

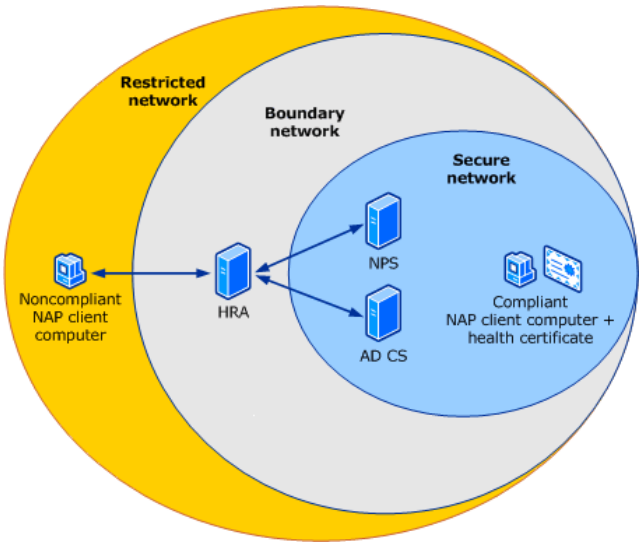

Figure 2 “Elements of IPsec Enforcement Design in Which Health Registration Authority (HRA), Network Policy Server (NPS) and Active Directory Certificate Services (AD CS) are running on separate networks”[12]

6. System Administrator (SA) Interface Requirements Analysis (17 requirements):

The SA requirements included the ability to specify versions and updates to: operating systems, applications, anti-virus and anti-spyware. They included the ability to limit access based on port, MAC and IP address. One requirement called for the SA to have two-factor authentication. Others addressed the ability to schedule vulnerability assessments at different time and audit those assessments.

6.1 Packetfence

The PacketFence open source product met 10 of the 17 requirements. This product relies on VLANS administered by system administrators to separate endpoint into normal (for registered and violation free endpoints), and isolation networks. This product is limited to basic functionality settings and it relies on third-party vulnerability scanning tools which can make configuration management complex. While the user interface was reportedly easy to use, the reports are limited. The administrator has a lot of flexibility; however, this open source product does lack some of the features of commercial products such as: defining a network policy, fine-tuning the assessments, authentication and reporting methods.[13] Examples of unmet requirements for Packetfence were: it did not allow for the administrator to schedule integrity assessments based on time or event, it did not allow the system administrator to override some settings and it did not support two-factor authentication.

6.2 Cisco

Cisco met 12 of the 17 requirements and has additional products that can be used to profile the prior to NAC implementation. This tool assists in identifying network assets, one of the difficult but foundational tasks in successful NAC fielding. Cisco does not have SA two-factor authentication or the ability to override some settings and audit that action.

6.3 Microsoft

Microsoft met 10 of the 17 SA requirements. It did not meet the ability to request granular reports, configure logging or contain two-factor authentication.

7. Authentication Requirements Analysis (42 Requirements)

Forty-two authentication requirements were further broken into the following categories: Endpoint (11), Verifier (11), Enforcer (4) and System (16). For each component, authentication requirements addressed the types of identifiers used (IP address, etc.) the authentication methods employed (public key infrastructure, username and password, etc.) and what authentication databases could be supported (Active Directory, Lightweight Directory Access Protocol (LDAP) etc.) In all three products, the verifier is not authenticated to the client.

7.1 PacketFence

The PacketFence open source product met 16 out of 42, did not meet 16 requirements and no evidence was found for 10 requirements. The authentication requirements contained some particular authentication server types such as RADIUS and Kerberos and whether or not users were also able to be identified by X.509 certificate. Therefore, PacketFence contains full authentication functionality, just not as many methods of authentication. For example, there is no support for PKI or 802.1x methods, thus PacketFence did not meet these two authentication requirements.

.

7.2 Cisco

Cisco met 33 out of 42 total authentication requirements. There were four requirements for which no evidence was found. The CISCO NAC product uses a free Clean Access Agent on the endpoint. Authentication can occur at either layer two or three. As mentioned in the Cisco product overview, authentication is not supported when EAP over UDP is used. The TPM is not used for CISCO authentication. Cisco integrates with a Cisco NAC module within their Integrated Services Routers and acts as an authentication proxy when used with Kerberos, RADIUS, Active Directory and other authentication servers. Role based access control was supported and Guest users can be authenticated via the Cisco Guest Server.

Cisco did well in this category because so many types of authentication are supported. It should be noted, however, that authentication is not mandatory and that differing levels of granularity can be implemented, creating either a robust or weak authentication mechanism.

7.3 Microsoft

Microsoft NAP met 21 of the 42 requirements, did not meet 8 and “no evidence in open literature” was noted for 13. Active Directory is used in the NAP authentication scheme and it can designate group as well as individual accesses. Both smart cards and Microsoft certificates containing user credentials can be used. Access is controlled via numerous methods of differing authentication strength. These are: 802.1x which provides a controlled port allowing access to the authenticator, or Dynamic Host Configuration Protocol (DHCP) which only issues IP addresses to compliant clients, and IPsec and VPN which control access based on encryption keys at the client. Many of the requirements not met were because of the lack of a consistent level of authentication strength and in some cases, lack of encryption of the authentication information.

8. Integrity Requirements Analysis (26 requirements)

There were a total of 26 integrity requirements further allocated to endpoint (3), system (12), verifier (3) and enforcement point (4). These requirements focused on the areas of integrity to be checked: operating system, software, and items under the Security Content Automation Protocol (SCAP) such as vulnerabilities and specific configurations. None of the products currently support the SCAP as content, which accounted for three integrity requirements.

The remediation function was also included under the Integrity topic. There were only four remediation requirements: repair, no repair and limited number of services, repair prior to any endpoint traffic traversing the network, and isolate the endpoint from the network. Based on continued study of NAC and remediation, some additional requirements that should be considered are: no communication between endpoints on the remediation network, and a verification scan before allowing remediated endpoints access to the network.

In order to trust the integrity measurements, the protocols should cryptographically connect the measurements to a root of trust for the client endpoints via the use of a TPM. This is not done, therefore, these solutions could contain a lying endpoint, or the integrity measurements may be subject to surreptitious change.

8.1 PacketFence

Of a total of 26 integrity requirements, PacketFence met 15, did not meet 9 and 2 were unable to be determined within open literature. PacketFence does not employ unique client software to check machine posture; instead, it supports external Nessus scanning and Snort detection. Nessus was an open source product by Tenable Network Security, Inc. Their open source product is now a less robust and user-friendly version of its proprietary product. Because PacketFence relies on these tools, there is a hierarchy of configuration management and updating that must be maintained. Lack of support or issues with third-

party products can affect PacketFence overall integrity performance. PacketFence did not meet the requirements in this section that called for the updating of integrity information, allowing an endpoint a limited set of services, determining the integrity of perimeter devices, and those supporting SCAP content.

8.2 Cisco

Of the 26 total requirements, Cisco met 16, did not meet 4 and had 6 that could not be determined by an open literature review. It does not make integrity evaluations of perimeter devices, and does not support Security Content Automation Protocol (SCAP) content.

Cisco offers automatic security policy updates and provides predefined policies for common network access criteria, critical operating system updates, software virus definition updates and anti-spyware definition updates.

Cisco's literature was the least detailed of the products reviewed for this paper and therefore, it was difficult to determine what integrity checks are accomplished and the exact decisions made. The granularity of the integrity checks and how often they get updated, etc. was not clear.[14] Cisco also integrates other vendors' products, requiring good configuration and life-cycle management. For remediation, the product blocks, isolates (either into a VLAN or a subnet) and then performs repairs.

8.3 Microsoft

Of the 26 total requirements in this section, Microsoft met 16, did not met 2, and 8 were unable to be determined by open literature. Microsoft NAP is very configurable, so the integrity settings are highly dependent on the system administrator settings and the overall corporate policy for governance of end clients. Microsoft did well with the integrity requirements and can provide essential information about platforms and applications running on those machines. NAP checks antivirus, anti-spyware and firewall settings and automatic updates but their policy enforcement is not as granular as some other products. For example, it does not control ports; time of day, etc. [15] NAP does handle unmanaged home computers and can verify their health state. However, it does this by the use of Active Directory Domain Services to control accesses and create a VPN connection.

9. Security Requirements Analysis (18 requirements):

All three products offer security "functionality" but do not make use of the Trusted Platform Module (TPM) as a hardware root of trust when communicating authentication and integrity data. This results in a lack of security for both the data content and the identity of the user and endpoint making the assertion.

Out of 18 total security requirements, Cisco met the most with 6 mostly because their literature spoke of encrypting inbound and outbound traffic. Both Microsoft and Packetfence only met two because they do not always enforce encryption and because the remaining security requirements focused on TPM functions such as storing the private key and platform integrity measures.

9.1 Packetfence

This product met two of the requirements but lacks a basis for trusting assertions made about the client status. The two requirements met were that it supports virtual private networks (VPNs) and performs authentication prior to DHCP traffic being passed.

9.1 Cisco

Cisco met 6 of the security requirements because their literature stated that encryption was used on inbound and outbound traffic. Cisco's NAC uses proprietary protocols which could mean that they have not been fully vetted and their security strength may not be well known or tested.

9.2 Microsoft

Microsoft met two of the security requirements. Because Microsoft offers different enforcement mechanisms for network access, it was difficult to rate the security requirements. While 802.1 x VLAN assignments are secure, for example, DCHP is not because it can be subverted by applying static IP addresses. If NAP is implemented by relying on IP address configuration enforcement, security is weak.

10. Functional Requirement Analysis (18 requirements):

This requirement set focused on confirmation messages, error messages, clear indications provided to users and administrators, support for both Internet Protocol Version 4 and 6 addressing, in-band and out-of-band implementation, multiple operating system support, managing un-owned devices and interoperability.

10.1 PacketFence

The functional requirement set focused on interfaces between components and the PacketFence product literature was not written at that detail. PacketFence can experience memory usage issues, especially with older machines. The VM appliance based PacketFence means that there is a sharing of resources with the host machine, therefore a large amount of memory is required. For an open source product, PacketFence did well, meeting 7 of the 18 functional requirements.

10.2 Cisco

Cisco met the most functional requirements (14) because their product sheets were very detailed. For example, they support both IPv4 and IPv6 addressing and operating system independence. At conferences and in some of the literature, indications were that fielding was complex, many choices to be made depending on the size and complexity of the network supported and the deployment mode chosen. Cisco did well in its ability to support IP connected devices such as phones and other

mobile devices. The four remaining requirements were unable to be determined by open literature.

10.2 Microsoft

A May 2009 article in InfoWorld magazine, rated NAP as fair in the areas of manageability, set-up and value.[16] In this analysis, NAP was found lacking in the reporting functions because it does not perform granular checks of integrity; it checks the status of anti-virus software, antispyware software, existence of a firewall and updating. Setting up supporting databases and services was mentioned as difficult. An all-windows environment is best when using this product.

11. Non-Functional Requirement Analysis (12 total requirements)

Non-functional requirements were difficult to analyze for this open literature based project because they needed to be measurable and include time and latency periods. The requirements included a "return-on-investment" item which all of the products "promoted" in their literature; the confirmation of that requirement would depend on customer implementation.

11.1 Packetfence

Two non-functional requirements were met; the first dealt with the response time of the network and the second was that the product allowed for incremental deployment. Five requirements were not met: scalable up to 5,000- client machines, network downtime, degradation of service and disruption to the operational environment and access time. Most of these related to the product installed on a virtual machine. Seven requirements were in the "unknown" category.

In the open literature reports, there is not much listed about non-functional measurements. Zen is for Zero Effort NAC, but the installation is not trivial.

11.2 Cisco

Cisco offers a "Network Admission Control" Implementation Service that can assist large enterprises in successfully implementing NAC. This systems engineering type service provides requirements analysis, and design and implementation consulting services. The company itself often promotes a limited, lab-environment deployment allowing the small-scale solution to define the requirements for a larger implementation. To assist with defining the network prior to NAC implementation, Cisco has developed a NAC Profiler component. Two requirements were confirmed as being met: incremental deployment possible and a return on investment can be achieved. Ten were listed as "unknown."

11.3 Microsoft

Microsoft met the incremental deployment requirement but the remaining 11 were in the "unknown" category.

While most other companies emphasize their ability to interoperate with numerous operating system platforms, Microsoft NAP literature does not mention this ability and technology magazines have noted that Microsoft does not support other operating systems. Customers want to manage a variety of endpoint types. In order to do this, they will need to integrate another product with NAP. This could become an issue as more and more consumers are managing mobility of their workforce.

12. Conclusion

This analysis of architectures and requirements resulted in seven security- related recommendations for NAC products and four implementation-related requirements.

12.1 Security Recommendations

NAC products should make use of the trusted platform module (TPM) as a hardware root-of-trust. This allows trust between NAC components that does not exist today. Current NAC components can be spoofed or subject to attacks from unauthenticated and unknown entities. A NAC component would be a good target for an adversary to impersonate in order to gain information about a network, its characteristics, software and possible weaknesses. A well-implemented, secure root of trust is a key element of NAC assurance that is missing in the products analyzed and in current deployments of NAC products. TPMs do exist in a large number of platforms but existing NAC applications do not make use of them. TPMs are delivered "turned off" based on Trusted Computing Group best practices. [17] Methods to deliver TPMs turned-on and to use them without physical presence assertions should be developed and deployed.

The TCG TNC system architecture and specifications should be analyzed and specific recommendations made to enhance security for NAC products. While the current specifications offer good advice and design guidance for interoperable communications, a security analysis of specific protocols could result in recommended security architecture for NAC products. Interoperability remains an important goal; proprietary solutions create barriers to an enterprise-wide deployment and to security functionality.

NAC verifiers should be required to authenticate to the end entity. Because this authentication is lacking, the end entity is responding blindly to a request for its integrity status. It could even respond favorably to the initiation of changes to its applications and software, accepting change requests from an un-authenticated entity.

NAC and its use of a TPM should be leveraged in the field of malware detection. NAC and the TPM can define a "known good state" and "known good software." The ability of the TPM to provide measurements of an endpoint pre-operating system environment should be utilized. NAC, together with trusted computing technology, can play an important part in moving the market away from ineffective detection of variants of malicious code that are appearing at a rate of approximately 8,000 new variants per day.[18]

As a part of the security analysis of TNC and NAC, special attention should be paid to the numerous access detection and authentication schemes. Some have known security vulnerabilities. The challenges of non-computer connected IP devices (phones, printers, etc.) often results in exceptions to network authentication policies. These exceptions can be used to defeat the authentication and provide unintended access. Administrative privileges are often overused within the NAC functionality suite creating vulnerabilities.

Align on-going multi-agency efforts to create common methods for enumerating configuration and vulnerability information with the TNC specification suite. Three agencies (National Institute of Standards and Technology (NIST), Department of Homeland Security (DHS), and the National Security Agency (NSA) have sponsored the creation of Secure Content Automation Protocol (SCAP) specifications which support machine-readable compliance checking of endpoints. A Common Vulnerability Scoring System (CVSS) was also completed. It is a method that is used to classify reported information and use it to provide scores related to systems and software. While NIST validated SCAP products exist today, the existing methods of transmitting the information across the network are all unique. TNC should be analyzed as the transport mechanism for SCAP content information. The TPM should be leveraged to create a trust foundation for SCAP and TNC.

The remediation functionality must be implemented securely so as not to create an environment where non-compliant clients infect each other. This may be easy to do on smaller local area networks but at an enterprise level may require a more sophisticated architecture within the remediation network. Review of the integrity and configuration at entry to the remediation network and a mandatory outbound inspection to ensure no additional problems have been encountered are recommended. In addition, no communication should be allowed between endpoints on a remediation network and the remediation network itself must have a secure architecture.

12. 2 Deployment and Implementation

NAC deployment should be done in carefully planned stages. NAC functionality should be partially deployed and that functionality measured for impact to the network. For example, authentication before connection can be monitored for a period of time prior to full implementation. Authentication by itself increases the security posture of a network. The integrity functions should be monitored initially in order to establish the use cases and policies best suited for the organization.

NAC must be implemented with keen awareness of what information has to be protected and what access policies are required. An analysis of existing access controls performed by endpoints and perimeter devices and the impact of adding NAC to the network is required. Existing products in use for anti-virus, anti-malware, intrusion detection and prevention and software updates may need to be integrated with the NAC solution. The solutions must be vetted carefully with IT staff because if seen as an additional burden or degradation to network performance, the IT staff may shut key security features down. Auditing should be re-evaluated to include NAC auditable events. NAC can improve life cycle management of an existing network and save man-hours by proactively ensuring endpoint integrity.

NAC requires the use of multiple network enclaves: pre-access, post access but remediation required, and a policy compliant network. VLAN containment can be used to achieve this architecture with access restricted by numerous methods of identifying the endpoint.

Pre-admission or post-admission is a choice for implementation. Should the network allow a user on, then check for integrity measures or deny access or limit access until integrity measures are determined? The most assured manner is to deny access until both authentication and integrity measures match the network policy.

13. References

[1] Trusted Network Connect (TNC) Architecture for Interoperability Specification Version 1.3, Revision 6 dated 26 April 2008

[2] Sangster, Paul, “Network Endpoint Assessment (NEA) Overview and Requirements”, RFC-5209 (no longer active), April 18, 2008, online at: https://datatracker.ietf.org/doc/draft-ietf-nea-requirements/

[3] Sangster, P., and K. Narayan, "PA-TNC: A Posture Attribute (PA) Protocol Compatible with Trusted Network Connect (TNC)”, RFC 5792, March 2010.

[4] Sahita, etal, “PB-TNC: A Posture Broker (PB) Protocol Compatible with Trusted Network Connect (TNC)” RFC 5793, March 2010

[5] Microsoft Technet, Windows Trusted Platform Module Management, Step by Step Guide, Online at: http://technet.microsoft.com/en-us/library/cc749022.aspx

[6] Schaeffer, Greg. “Jumping into open source NAC with PacketFence ZEN” Computerworld , May 21, 2007, Online at: http://www.computerworld.com/s/article/9020219/Jumping_into_open_source_NAC_with_PacketFence_ZEN

[7] Davis, David. “Get familiar with Cisco’s NAC solution, “ dated Dec 6, 2007, online at: http://articles.techrepublic.com.com/2415-1035_11-178688.html

[8] “Cisco Network Admission Control and Microsoft Network Access Protection Interoperability Architecture,” Microsoft and Cisco Corporations, published September 2006, online at: download.microsoft.com/download/.../NAC-NAP_Whitepaper.pdf

[9] "Cisco NAC Network Module for Integrated Services Routers" Product data sheet, no date, online at: http://www.cisco.com/en/US/prod/collateral/modules/ps2797/ps8788/product_data_sheet0900aecd806bfe24_ps5854_Products_Data_Sheet.html

[10] Interop Labs "What is Cisco NAC," May 2006, online at: http://www.interop.com/archive/pdfs/CISCONAC.pdf

[11] Microsoft Technet "Mapping Your Deployment Goals to a NAP Design" October 6, 2008, online at: http://technet.microsoft.com/en-us/library/dd125346(WS.10).aspx

[12] Microsoft Technet "IPsec Enforcement Design," October 6, 2008, online at: http://technet.microsoft.com/en-us/library/dd125391(WS.10).aspx

[13] Balzard, Regis and Gehl, Dominik. "Packetfence Revisited" Linux Journal, January 1, 2008, Online at: http://www.linuxjournal.com/article/9894

[14] Cisco Network Admission Control Executive Overview Online at: http://www.cisco.com/en/US/solutions/collateral/ns340/ns394/ns171/ns466/net_implementation_white_paper0900aecd80557152.html

[15] InfoWorld Staff, Steven Hultquist "Microsoft NAP: NAC for the Rest of Us?" InfoWorld May 14, 2009 Online at: http://www.infoworld.com/print/75294

[16] InfoWorld Staff. "Microsoft NAP: NAC for the Rest of Us?" InfoWorld May 14, 2009, online at: http://www.infoworld.com/print/75294

[17] "TCG Design, Implementation and Usage Principles (Best Practices), Version 2.0, December 2005, Online at: http://www.trustedcomputinggroup.org/files/resource/files/59C26ECB-1D09-3519-AD469EA7AF8D2E91/Best_Practices_Principles_Document_V2_0.pdf

[18] Jackson, William "Count to Eight, Say Hello to a New Malware Signature," Government Computer News, July 13, 2009,

14. VITA

Gloria Serrao is in the Senior Technical Development Program at the National Security Agency (NSA) studying network access control and its use in securing DoD and U.S. Government networks.

Gloria holds a Bachelor of Science Degree in Computer Science from the University of Maryland, University College and recently graduated (May 2010) from Stevens Institute of Technology with a Master of Engineering Degree in Systems Engineering.

This paper is a condensed version of her Masters' degree project completed under the mentorship of Professor William Miller at Stevens Institute of Technology.