

Assessing Trusted Network Access Control Cost-Benefit Factors ¹

Susmit Panjwani and Stephanie Tan

Deviant Intelligence, LLC
Gaithersburg, MD 20878
susmit[at]gmail.com

Deviant Intelligence, LLC
Gaithersburg, MD 20878
stephanie.tan[at]gmail.com

Abstract

“Organizations spend millions on security products and services but leave the responsibility of installing and updating these critical security measures in the hands of users, expecting most users to voluntarily comply.”² This may impact the security infrastructure adversely. This becomes a major problem in maintaining the security posture of the computing devices. Organizations may choose to alleviate this problem by acquiring solutions that mandate the compliance with the organization’s security implementation and change management policy. Different cost-benefit factors associated with voluntary and mandatory compliance are assessed using the Trusted Network Access Control framework.

Keywords:

NAC, Network Access Control, Trusted Computing, Investment Analysis, Cost-benefit factor analysis.

¹ This paper illustrates the author’s independent research and does not represent the work done at the author’s organization affiliation.

² Meeting Network Security Gaps http://www.endforce.com/pdf/Meeting_Network_Security_Gaps.pdf

1 Introduction

“Organizations spend millions on security products and services but leave the responsibility of installing and updating these critical security measures in the hands of users, expecting most users to voluntarily comply” [1]. Oftentimes, there is little or no enforcement mechanism in place to drive compliance and report compliance results². Hence, the organization’s security state is a function of the user diligence in maintaining the security posture of their devices.

One of the manifestations of this problem can be observed in an organization’s network access policy. Organizations acquire security tools such as the anti-virus, personal firewall systems, operating system and patch management software, etc. These tools are then distributed to all users hoping the safeguards will keep computing devices safe from threats including automated attacks like worms and viruses. The effectiveness of these tools rely on the latest installed attack signatures and the security updates. Unfortunately, installations of these security tool updates are left to the user’s discretion. Moreover, organization users are increasingly mobile and the same computing device (e.g. a laptop) is frequently used in many network infrastructures, ranging from the local coffee house to the organization’s protected network. As a result, a non-compliant computing device, without updated detective capabilities like the latest anti-virus signature or preventive capabilities like operating system or application security updates, may get infected from an unprotected network and spread the attacks upon entry to the organization’s protected network boundary.

Organizations can either use a reactive or a proactive approach. In a reactive approach, users voluntarily update security tools and organizations use detective technologies like intrusion detection systems to detect infected computing devices. In a proactive approach, organizations use Trusted Network Access Control (TNAC) to determine the security posture of the computing devices prior to organization network entry.

This paper discusses the cost-benefit factors of and the proactive TNAC approach. Section 2 discusses the background of the network access problem in detail. Section 3 introduces the state of technology available to solve this problem. Section 4 illustrates the cost benefit drivers of the network access technology. Finally, section 5 concludes the paper and describes the future work.

2 Background

The basic perception of an attack is malicious behavior from an entity outside the network perimeter of the victim organization [2]. As a result, security tools are often deployed at the network perimeter [3] [4]. In reality, attacks can originate from within the network boundary. Attacks from within the organization can result from malicious intents of an attacker in which the attacker knowingly launches an attack or as a result of ignorance from a non-malicious user who unknowingly puts an infected computing device inside the organization's network boundary. The non-malicious user's infected computing device spreads infection through automated attacks within the network. Though capable of detecting automated attacks, network perimeter security tools do not catch attacks *inside* the network since the original computing device is already inside the network boundary. Furthermore, even if the infected computing device is later removed from the network, the infection still persists among other computing devices in the network.

Two solutions to this problem involve reactive or proactive approaches. For the reactive approach, security administrators reconfigure the security architecture to include more security tools like intrusion detection sensors within the organization boundary for faster detection of infected host computing devices. However, attacks like worms propagate substantially before security alerts are observed and the infected computing device is located. This is a major problem for organizations with a large number of computing devices.

A proactive approach is using Trusted Network Access Control (TNAC). In TNAC, any computing device requesting access to the network is evaluated to determine the security posture or the security level of the machine. This security posture is then compared with the organization's network access policy for a computing device's minimum security posture prior to being granted network access. After this initial "scan-and-block", a term coined by Gartner Research, the network access control process also provides "means for mitigation of non-compliant devices, monitoring of changes in device security state and network activity, containment of any infected devices in order to minimize the threat to the network, and maintenance of the network's original security through proper configuration management" [1]. Organizations need to evaluate the return on investment from this proactive approach. According to Gartner Research, 80 percent of enterprises will have implemented network access control policies and procedures by year-end 2007 [5].

Several TNAC technologies are already available or currently under development. Major technologies include the Trusted Computing Group's Trusted Network Connect

[6], Microsoft's Network Access Protocol [7], and Cisco's Network Admission Control [8].

3 TNAC Introduction and Approaches

TNAC at its core is a simple concept: "Who you are should govern what you're allowed to do on the network" [9]. TNAC is an architecture that lets organizations enforce network access control policies based on "who you are."

In order to better understand the TNAC better let's look at what TNAC is not.

What TNAC isn't?

- Although a TNAC could be as simple as a "go/no-go" decision on network access, it provides a capability that is much more extensive than simple access control.
- A good TNAC product is not simply a way to flip users between quarantine and production networks.
- TNAC is different from control systems such as firewalls.

What TNAC really is?

TNAC is a generic access control system that authenticates and authorizes all network traffic based on user credentials and the system security posture, while also providing capabilities to remediate problems that might restrict users from accessing network resources. As a result, TNAC has three core functionalities that are summarized as below.

1. Authentication

This authentication is done on the basis of

- Who is accessing the network? This deals with user-level authentication.
- How the user is requesting access? This deals with the user's access method (e.g. LAN connection, VPN tunnel, Wireless 802.11, etc).
- What the users are using to access the network? This deals with the security posture of the computing device.

2. Authorization

Once the users and computing devices are authenticated using the authentication scheme mentioned above, TNAC determines whether to grant full, partial or no access to the user and or the computing device. This decision is based on the organization's network access policy. If users have sufficient credentials for accessing network resources but the computing device does not match the organization's security posture requirements, users are directed to remediation systems and/or processes. For example, if a connecting computing device does not have the standard corporate anti-virus package and latest signatures, the user should be granted a different access control policy than if everything is installed and all virus signatures are up-to-date.

3. Remediation

This can be a system or a process that upgrades the security posture of a computing device that failed to meet the minimum security posture requirement of the organization's network access policy. The remediation process may entail updating the anti-virus, installing latest security patches, etc.

4 Cost-Benefit Factor Analysis

This section analyzes the factors that can incur cost and generate benefits. Hypotheses are formulated and used as a basis of the investment decision. These hypotheses do not make

any assumption regarding the organization infrastructure or a specific TNAC technology being considered for investment. Note that the actual benefits will depend on the organization structure, the nature of business, and the TNAC solution. Decision makers can use these hypotheses as the basis for building the hypotheses relative to their own organization structure. Furthermore, important cost-benefit factors that impact these investment hypotheses are described in the five phases of the TNAC solution lifecycle,

4.1 Problem Determination Phase: NAC Cost Benefit Drivers

In the Problem Determination Phase, one determines if this is a problem worth alleviating. A decision to consider investing in the solution may or may not be made at this stage depending on the severity of the problem (or the strength of the investment drivers). The decision in this phase is based on qualitative data and analysis should not be extensive due to the opportunity cost associated with a comprehensive analysis. The basic investment drivers that instigate the need for a technological solution are determined. The basic investment drivers can be classified into three main categories: threats, business requirements and business opportunity. Some of these drivers are intuitive in nature but they are crucial for the investment decision as they will determine the benefits that can be achieved from the use of the technology.

Threats:

As previously discussed, the main threat that TNAC can alleviate is the number of malicious activity attacking the organization network from the inside as well as outside. Hence, the benefit of the TNAC technology will be the amount saved 1) by preventing the loss in confidentiality, availability and integrity (CIA) of the infected computing

devices, 2) the amount spent on remediation or replacement of the infected computing devices, and 3) the opportunity cost of not using the infected system.

Business Requirements:

The current state of technology has changed the way organizations do business. Users can now access the organization's computing resources from virtually any location in the world. It is the organization's responsibility to provide these users with secure and uninterrupted access to the computing resources. Conversely, organizations should protect its computing resources from unauthorized access and accidental or intentional data corruption, which affect confidentiality and integrity. Furthermore, it is a challenging task to enforce security policies like anti-virus and patch updates on the mobile users. It is a major business requirement to design a network access mechanism that can provide users with 24/7 access to computing resources while integrating security.

Business Opportunity:

The proliferation of offshore development, outsourcing and B2B alliance in present day business environments provide organizations an opportunity to focus on their core competencies. This business opportunity presents the problem of establishing an organizational level trust between the partner organizations. Often these organizations need to communicate with partner organizations over a network. It is imperative that the host organization design a trusted network that allows partner organizations access to computing resources on a need-to-know basis while protecting the CIA of the host organization's network infrastructure.

Table 1 Technology Drivers and Benefits

Drivers	Benefits from technology
Threats	1) Amount saved by preventing the loss in confidentiality, availability and integrity of infected computing devices. 2) Amount spent on remediation or replacement of infected computing devices. 3) Amount lost due from the opportunity cost of not using infected computing devices.
Business Requirement	1) Increase in efficiency by providing the uninterrupted access to organizational users throughout the world.
Business Opportunity	1) Establishing the requirements for mutual trust in network access policies to protect the confidentiality, availability and integrity.

Alleviating threats have immediate benefits and are the easiest factors to quantify.

Conversely, business requirements and opportunity factors have long-term benefits and are difficult to quantify but should be the driving factors for investment decisions.

4.2 Requirements Phase: Basic Investment Hypothesis

Once the problem is identified, the extent of the problem is determined and defined in the problem space. Basic investment hypotheses are formed and preliminary data is collected in order to evaluate and predict the cost-benefit of the TNAC solution. These hypotheses are derived from the cost benefit drivers. For building these hypotheses, focus should be on the costs and benefits in the Operations Phase because 1) the actual benefits are gained only after the TNAC solution is in operation 2) this paper limits the focus on the cost-benefit factors specific to the TNAC solution only. Since TNAC is a software solution, the product lifecycle costs can be evaluated by mapping the TNAC software to lifecycle cost estimation guidelines like [10] [11] [12].

The outcome of this phase is 1) the decision to invest in the solution if no decision was made at the end of the problem determination phase and 2) the requirements for the TNAC solution.

4.2.1 Hypotheses related to benefits

TNAC increases confidentiality of data

TNAC can increase the confidentiality level of an organization's data by reducing the frequency and the severity of security breaches. The losses that TNAC can alleviate include the unavailability of the financial information to the investors, unavailability of the organization's primary website, unauthorized disclosure of critical information, permanent loss of critical organization data, etc. Note that TNAC can only alleviate the losses due to automated attacks like worms and viruses. The impact of such losses are difficult to measure quantitatively and are generally determined by upper-level management. The benefit gained by using TNAC is equal to the amount saved from the expected losses due to the threat of the automated attacks. For measuring these expected losses, upper-level management needs to determine the probability of occurrence of a threat due to automated attacks and the potential amount lost if such threat is realized. Upper-level management must work with the IT department to determine the percentage of threats from automated attacks.

$$B_{conf} = L_{conf} * E_{TNAC} \quad (1)$$

Where

B_{conf} = Expected Benefit due to implementation of TNAC

L_{conf} = Expected Loss in confidentiality without the implementation of TNAC

E_{TNAC} = Efficiency of TNAC in reducing the threat due to automated attacks

If the TNAC solution is able to alleviate threats due to automated attacks completely, then expected benefits would be equal to the expected loss. However, TNAC deals only with alleviating the attack threats from a computing device in the organization network (physically or logically).

TNAC increases productivity

IT support staff productivity increase

TNAC increases IT support staff productivity by decreasing the amount of time required to locate, patch and test infected computing devices. This can be measured by the following formula.

$$B_{ISS} = (T_{loc} + T_{patch} + T_{test}) * F_{inf} * A_{support} \quad (2)$$

Where

B_{ISS} = Benefit gained from increase in productivity of IT support staff

T_{loc} = Time to locate the infected computing device in hours

T_{patch} = Time to disinfect and patch the infected computing device in hours

T_{test} = Time to test the patched computing device in hours

F_{inf} = frequency of infection

$A_{support}$ = IT support staff hourly rate in dollars

In this formula, the IT support staff salary is considered as the opportunity cost of locating, patching and testing the infected computing device. Note that this

opportunity cost may be higher if the support staff has competing priorities (e.g. working on other projects that yield higher benefits).

Mobile user productivity increase

TNAC increases the productivity of mobile users by decreasing the computing devices downtime due to automated attack threats and decreasing the loss in efficiency due to infected computing devices. The downtime of the computing device comprises of the scenario when the device is unusable due to infection or the case in which the device is put in a quarantine network. Also, automated attacks like malware and adware decrease the performance of the computing device significantly and decrease the efficiency of the user. TNAC alleviates this problem by minimizing the probability of infection through network entry security posture enforcement. The benefit from TNAC in the case of mobile user productivity increase is given below.

$$B_{MU} = (F_{mu_uavail} * A_{dt} * C_{uavail}) + (E_{infection} * F_{infection} * C_{mu}) \quad (3)$$

Where

B_{MU} = Benefit obtained by increase in productivity of the mobile user.

F_{mu_uavail} = Frequency of downtime incidents

A_{dt} = Average downtime due to automated attacks in hours

C_{uavail} = Opportunity cost of the unavailability of the device in dollars

$E_{infection}$ = Decrease in efficiency due to infection from automated attacks (e.g. malware)

$F_{infection}$ = Frequency of infection from automated attack incidents

C_{mu} = Mobile user hourly rate in dollars

TNAC increases end-user productivity

TNAC increases end-user productivity by decreasing the downtime of computing resources. The benefit from end-user productivity increases can be measured as given below.

$$B_{OU_Avail} = F_{srv_uvail} * (A_{srv_dt} * C_{uvail} * N_{users} + C_{remediation}) \quad (4)$$

Where,

B_{OU_Avail} = Benefit obtained by increase in user productivity by increasing availability of computing resources.

F_{srv_uvail} = Frequency of computing resource downtime incidents

A_{srv_dt} = Avg. downtime of computing resource due to automated attacks

C_{uvail} = Opportunity cost of the unavailability of computing resources in dollars per hour

N_{users} = Number of users using the computing resources

$C_{remediation}$ = Cost of remediation in dollars per hour

The cost factor for remediation assumes that a remediation is possible. TNAC also can protect the organization from corruption and loss of data due to automated attacks. This can be quantified as

$$B_{OU_Data} = C_{regen} * + C_{uvail_data} \quad (5)$$

Where

B_{OU_Data} = Benefit obtained by increase in productivity of the organization users by increasing the integrity of data

C_{regen} = Cost of regenerating the data

C_{uvail_data} = Opportunity cost of unavailability of data

Assumption: Lost data can be regenerated. Generally, crucial data are regularly backed up as a part of the organization's contingency plans.

TNAC increases security awareness

The TNAC process increases user security awareness due to the implications of non-compliance. As a result, user diligence increases because the computing device's security posture must be maintained. The increase in user awareness may mitigate some of the losses due to automated attacks. Typically, this is a subjective assessment and is generally measured qualitatively.

TNAC increases the level of B2B trust

TNAC allows organizations to build a framework for establishing mutual trust in B2B transactions. The benefit gained by this depends on the organization's infrastructure and nature of business. This is evaluated subjectively by upper-level management.

TNAC helps establish accountability

Network access control security logs can store the security posture of computing devices trying to access the organization network. The security posture information of the computing devices can be used to determine the root-cause of internal automated attack propagation. The actual benefit of the increase in accountability depends on the organization security policies and guidelines and varies from organization to organization.

The total operational benefit of the TNAC solution is given below.

$$B_{total} = B_{conf} + B_{OU_Data} + B_{OU_Avail} + B_{ISS} + BMU + B_a + B_t + B_{acc} \quad (6)$$

Where,

B_a = Benefit in terms of the amount saved due to increase in awareness

B_t = Benefit in terms of the amount saved due to increase in B2B trust

B_{acc} = Benefit in terms of the amount saved due to increase in accountability

4.2.2 Hypotheses related to costs

TNAC increases the cost of policy management

TNAC is a policy driven solution and hence the strength of the solution depends on the strength of the security policy. As a result, the TNAC increases the time for policy management. This is measured as

$$C_{pm} = F_{update} * T_{update} * C_{update} \quad (7)$$

C_{pm} = Cost of TNAC policy management

F_{update} = Frequency of the policy update needed

T_{update} = Time required to update the policy

C_{update} = Cost of policy maintenance measured in the policy manager's hourly rate in dollars.

TNAC increases maintenance costs

TNAC increases maintenance costs since additional systems need to be implemented in order to use the solution. This is measured as follows.

$$C_{main} = N_{sys} * T_{main} * C_{admin} \quad (8)$$

C_{main} = Maintenance Cost of TNAC

N_{sys} = Number of systems requiring maintenance

T_{main} = Time required for maintenance

C_{admin} = Cost of maintenance measured in the system administrator's hourly rate in dollars.

TNAC decreases the productivity of non-compliant users

TNAC may decrease non-compliant user productivity since users may need to go through the remediation process. This increases the time to access the network for a non-compliant user. This can be estimated as follows.

$$C_{prod} = T_{access} * C_{uvail_asset} \quad (9)$$

C_{prod} = Cost of loss in productivity of non-complaint user

T_{access} = Increase in Time to access

C_{uvail_asse} = Opportunity cost of unavailability of the asset

The total cost can be given as

$$C_{total} = C_{pm} + C_{main} + C_{prod} \quad (10)$$

These costs and benefits are summarized in Table 2 Costs and Benefits.

Table 2 Costs and Benefits

Hypothesis	Impact	Measurement of Impact
TNAC increases confidentiality of data	Reduction in the frequency and the severity of security breaches affecting confidentiality	Amount saved from expected losses due to the threat of automated attacks.
TNAC increases IT Support staff productivity	Decrease in the amount of time required to locate, patch and test the machines.	(Time to locate + Time to patch + Time to test) * frequency of infection * Salary of IT support staff in \$ per hour
TNAC increases mobile user productivity	Decreases the downtime of end-user devices	Frequency of downtime incidents * Avg. downtime due to automated attacks in hours * opportunity cost of the unavailability of the device in dollars
	Decrease the loss due to decrease in efficiency of the end-user device	Frequency of infection from automated attacks * Decrease in efficiency due to infection * Salary of the mobile user in \$ per hour.
TNAC increases end-user productivity	Decrease in downtime of the servers and other IT resources	Frequency of downtime incidents * (Avg. downtime of servers due to automated attacks * number of users using the servers * opportunity cost in \$ per hour of the + remediation process \$ per hour)
	Protects the data against corruption and loss	Cost of rebuilding the data + Opportunity cost of data unavailability
TNAC increases security awareness	Organization users are more aware of the security implications of non-compliance	Benefits gained from increase in awareness
TNAC increases the level of B2B trust	TNAC allows organizations to build a framework for establishing mutual trust in B2B transactions	Benefits gained from establishment of B2B trust based access control.
TNAC helps establish accountability	The security state logs of the devices can be used to determine the root-cause of internal automated attack propagation.	Benefits gained from increase in accountability
TNAC increases the cost	Increase in the time for policy management	Frequency of the policy update needed * Time required to update the policy * Policy manager's salary in \$ per hour
	Increases the maintenance cost	Number of systems requiring maintenance * Time required for maintenance * System administrator's salary in \$ per hour
TNAC decreases non-compliant user productivity	Increases the time to access the network for non-compliant users	Increase in Time to access * Opportunity cost of unavailability of the asset

The factors identified in this section can be evaluated quantitatively by analyzing organization historic security trends or qualitatively using expert opinions. Once these factors are quantified, a preliminary investment assessment can be made by using following formula.

$$B_{inv} = B_{total} - (C_{est_impl} + C_{req} + C_{est_sel} + C_{total}) \quad (11)$$

Where

B_{inv} = Total benefit from investment in the TNAC solution

B_{total} = Estimate of benefits gained in the operations phase

C_{est_impl} = Estimate of the implementation cost

C_{req} = Cost of performing the requirements study

C_{est_sel} = Estimate of cost to select the product

C_{total} = Estimate of cost associated with the operations phase

As previously discussed, this paper focuses on the operational costs and benefits specifically for TNAC. The cost of implementation, requirements, and selection can be modeled by using other software cost estimation techniques [10] [11] [12].

4.3 Selection Phase: Determining the Efficiency of the Tool

The Selection Phase comprises of activities like the selection of the TNAC technology from available solutions, establishing the necessary performance indicators for the solution, and determining policies and guidelines for the TNAC. The prominent TNAC solutions include Trusted Computing Group's Trusted Network Connect, Microsoft's Network Access Protocol and Cisco's Network Admission Control solution. The problem space definition in the Requirements Phase drives the necessary performance indicators (efficiency) for the TNAC product. The necessary performance indicators are the ability of the TNAC solution to alleviate the problems identified in the problem space. This is measured in terms of the percentage of the problem space the TNAC

product solves. This phase updates the investment assessment made at the end of the Requirements Phase with the estimated efficiency.

This section describes how the efficiency may affect investment equations 1-5 described in section 4.2.1.

- The expected benefit from the TNAC solution depends on the Efficiency of the TNAC solution on providing protection against automated attacks.

$$B_{conf} = L_{conf} * E_{TNAC}$$

- The frequency of infection described in equation 2 $\{ B_{ISS} = (T_{loc} + T_{patch} + T_{test}) * F_{inf} * A_{support} \}$ is a function of the efficiency of the TNAC solution. More precisely, the frequency of the reduction in attacks can be obtained by

$$F_{red} = F_{inf} * (1 - E_{inf}) \quad (12)$$

Where

F_{red} = Reduction in the frequency of infections

E_{inf} = Efficiency of the TNAC solution to reduce the frequency of infections

- The frequency of downtime incidents (F_{mu_uvail}) and the frequency of automated attack infections are also the function of the efficiency of the tool on reducing the downtime and reducing the number of automated attack incidents $B_{MU} =$

$$(F_{mu_uvail} * A_{dt} * C_{uvail}) + (F_{infection} * E_{infectione} * C_{mu})$$

$$F_{red_infection} = F_{infection} * (1 - E_{inf_infection}) \quad (13)$$

$$F_{red_mu_uvail} = F_{mu_uvail} * (1 - E_{inf_mu_uvail}) \quad (14)$$

where

$F_{red_infection}$ = Reduction in the frequency of infection

$E_{inf_infection}$ = Efficiency of the TNAC solution to reduce the frequency of infection

$F_{red_mu_uvail}$ = Reduction in the frequency of user device downtime

$E_{inf_mu_uvail}$ = Efficiency of the TNAC solution to reduce the frequency of user device downtime

- Similarly, the frequency of the server (F_{srv_uvail}) downtime in equation 4 is also a function of the efficiency of the tool $B_{OU_Avail} = F_{srv_uvail} * (A_{srv_dt} * C_{uvail} * N_{users} + C_{remediation})$

$$F_{red_srv_uvail} = F_{srv_uvail} * (1 - E_{inf_srv_uvail}) \quad (15)$$

Where

$F_{red_srv_uvail}$ = Reduction in the frequency of server downtime

$E_{inf_srv_uvail}$ = Efficiency of the TNAC solution to reduce the server downtime

- The frequency of unavailability of data from equation 5 can be updated accordingly. $B_{OU_Data} = F_{uvail_data} (C_{regen} * + C_{uvail_data})$

$$F_{red_uvai_data} = F_{uvai_data} * (1 - E_{uvail_data}) \quad (16)$$

Where

F_{uvail_data} = Reduction in the frequency of corruption of data

E_{uvail_data} = Efficiency of the TNAC solution to reduce the corruption of data.

- The benefit in terms of the amount saved due to increase in awareness (B_a), B2B trust (B_t), and accountability (B_{acc}) is not affected by the efficiency of the tool.

After incorporating the efficiency of the tool in to equations 1-5 using equations 12-16, the post-selection investment can be calculated using following equation

$$B_{ps_inv} = (B_{ps_conf} + B_{ps_OU_Data} + B_{ps_OU_Avail} + B_{ps_ISS} + B_{ps_MU}) - (C_{est_impl} + C_{req} + C_{sel} + C_{total}) \quad (17)$$

Where

C_{sel} = Actual cost encountered in selection phase

4.4 Implementation Phase: Determining Loss in Efficiency

The Implementation Phase is the main cost driver. This paper does not focus on the cost factors in the investment phase but rather focuses on the outcome of the investment phase. Risks during the Implementation Phase include the challenges in meeting necessary performance indicators due to unforeseen workarounds required to install the solution in a specific environment. This can also result from conflicts between the solution and other products in the organization.

The loss in efficiencies can be updated to include risks during the Implementation Phase (e.g. unforeseen workarounds) by multiplying E_{TNAC} , E_{inf} , $E_{inf_infection}$, $E_{inf_mu_uvail}$, $E_{inf_srv_uvail}$ and E_{uvail_data} with $(1-L_{TNAC})$, $(1-L_{inf})$, $(1-L_{inf_infection})$, $(1-L_{inf_mu_uvail})$, $(1-L_{inf_srv_uvail})$ and $(1-L_{uvail_data})$ respectively.

Equation 17 can be updated to calculate the post-implementation benefits

$$B_{pi_inv} = (B_{pi_conf} + B_{pi_OU_Data} + B_{pi_OU_Avail} + B_{pi_ISS} + B_{pi_MU}) - (C_{impl} + C_{req} + C_{sel} + C_{total}) \quad (18)$$

Where

$L_{TNAC} = \text{LOSS in } E_{TNAC},$

$L_{inf} = \text{LOSS in } E_{inf},$

$L_{inf_infectione} = \text{LOSS in } E_{inf_infection},$

$L_{inf_mu_uvail} = \text{LOSS in } E_{inf_mu_uvail},$

$L_{inf_srv_uvail} = \text{LOSS in } E_{inf_srv_uvail}$

$L_{uvail_data} = \text{LOSS in } E_{uvail_data}$

$C_{impl} = \text{Actual cost encountered in implementation phase}$

4.5 Operations Phase

The actual benefits are not derived until the Operations Phase and are also contingent on the successful implementation of the solution. All previous phases identify major costs and minimal benefits. However, this phase measures the actual production efficiency of the tool (performance indicators). Note that the efficiency of the TNAC solution is an important variable and fluctuation in this variable may have significant impact on the return on investment. Additionally, the attack threats and vulnerability profiles change over time thus affecting the efficiency of the TNAC solution. Consequently, the efficiency of the tool for its entire life cycle needs to be continuously measured during the Operations Phase in order to determine if the efficiency of the tool falls below the minimum profitable efficiency.

5 Conclusion and Future Work

Organizations acquire and distribute security tools hoping the safeguards will keep computing devices safe from threats including automated attacks. The installation and maintenance of these tools and their security signatures are left to the user's discretion. Moreover, organization users are increasingly mobile making a non-compliant computing device more vulnerable to attacks since detective and preventative capabilities are not up-to-date.

Organizations can either use a reactive or a proactive approach to alleviate this problem. In this paper we discuss the cost-benefit factors of the proactive TNAC approach. We identified the cost-benefit drivers and hypotheses which drive the investment decision. We identify the efficiency of the TNAC solution is the driving factor to determine the return on investment. This efficiency changes over the lifecycle of the solution. It is crucial to measure the change in efficiency due to the impact of the selection, implementation and operations life cycle phases.

We need organization specific data to quantify the parameters identified in this paper and propose to use a case study based approach to collect this data. Moreover, the major TNAC technologies described in this paper, like Trusted Computing Group's Trusted Network Solution and Microsoft's Network Access Protocol, are still under development. A further in-depth evaluation of the investment in TNAC can be performed upon availability of these products.

6 References

- [1] "Meeting Network Security Gaps at Industry and Enterprise Levels." Endforce (2005) 21 Oct 2006
<http://www.endforce.com/pdf/Meeting_Network_Security_Gaps.pdf>.
- [2] Tittel, E. CISSP: Certified Information Systems Security Professional Study Guide. Sybex Inc, 2003.
- [3] Koziol, J. Intrusion Detection with Snort. 2. Sams, 2003.
- [4] Ogletree, Terry. Practical Firewalls. 1. Que, 2000.
- [5] Nicolett, M. et al. "Implement a Network Access Control Architecture." 1 December 2004. <www.gartner.com>.
- [7] "Network Access Protection Platform Architecture." Microsoft 23 May 2006 21 Oct 2006
<<http://www.microsoft.com/technet/itsolutions/network/nap/naparch.msp>>.
- [6] "Trusted Computing Group: Trusted Network Connect." 2006. Trusted Computing Group. 21 Oct 2006
<<https://www.trustedcomputinggroup.org/groups/network/>>.
- [8] "Network Admission Control - Cisco Systems." 2006. Cisco. 21 Oct 2006
<http://www.cisco.com/en/US/netsol/ns466/networking_solutions_package.html>.
- [9] "What is NAC?." Interop Labs May 2006 21 Oct 2006
<<http://www.opus1.com/nac/2006whatisnac.pdf>>.
- [10] Reifer, Donald. "A model for Estimating the Cost of Securing the Network Infrastructure and Anti-tamper." WEIS 2006:
- [11] "Barry Boehm." University of Southern California. 21 Oct 2006
<<http://sunset.usc.edu/people/barry.html>>.
- [12] "Publications and Reports." University of Southern California. 21 Oct 2006
<http://sunset.usc.edu/publications/publications_main.html>.