Measuring security in a grid computing environment

Jørgen Belsaas

Master's Thesis
Master of Science in Information Security
30 ECTS
Department of Computer Science and Media Technology
Gjøvik University College, 2005

The MSc programme in Information Security is run in cooperation with the Royal Institute of Technology (KTH) in Stockholm.

Institutt for
informatikk og medieteknikk
Høgskolen i Gjøvik
Postboks 191
2802 Gjøvik

Department of Computer Science
and Media Technology
Gjøvik University College
Box 191
N-2802 Gjøvik
Norway

Abstract

In the world of today computer and network systems are growing larger and more complex to support the computational needs we face. An important issue when working with a complex system, is the security of the information processed within. This is especially true if personally identifiable information, or other private information, is being processed. Preferably we would want to measure the security, and get a simple number which expressed the level of security, but this is not always possible.

One system which is told to be the future of the information technology industry is grid computing. Grid computing is generally joining networks and computational facilities into a big computational environment. The result of such a joining is usually a large and complex network, where it is difficult to follow the outline of security implemented. To get an outline, and even measure the level of security one needs a tool. One tool for this may be security metrics.

This thesis takes a look at grid computing, and at what vulnerabilities one might face when using a grid. A look at what may be used to eliminate these vulnerabilities is also presented. In this thesis the vulnerabilities and security measures are used to define a set of security metrics. These metrics may be used to map the vulnerabilities of the grid computing network, measuring the security, and pin down what actions needed to be taken to eliminate the vulnerabilities one faces.

An overview of the usage of the metrics defined in this thesis is included, both to show the fact that these metrics may be used to measure a running grid, and to get some test data. The test data are used to present how one can measure the distance between, and classify, the different security configurations. This may be used to find balance between needed security and needed efficiency of the grid computing network.

Sammendrag (Abstract in Norwegian)

Data og nettverkssystemer blir stadig større og mer komplekse siden nye krav til hastighet og kapasitet dukker opp. Informasjonssikkerheten i et slikt system er ofte viktig, spesielt hvis informasjonen som behandles er personopplysinger eller annen privat informasjon. Aller helst skulle man få målt sikkerheten i systemet og gjerne satt ett tall på hvor sikkert det er, men dette er ikke alltid mulig.

Gridsystemer sies å være det som vil behandle store mengder av data i fremtiden. Dette går generelt ut på å samle flere nettverk og systemer til et stort system for å gjøre behandling av data mer effektivt. Når man slår sammen flere nettverk og systemer til et stort virtuelt system, fører dette gjerne til at systemet også blir komplekst. Å få en oversikt over hvilke sårbarheter man står ovenfor, eller hvor sikkert systemet er kan være vanskelig, med mindre man har et verktøy til å hjelpe seg. Et verktøy man kan bruke er sikkerhetsmetrikker.

Denne rapporten ser på grid computing, og de sårbarheter man gjerne står ansikt til ansikt med når man bruker et gridsystem. En del sikkerhetstiltak som kan brukes for å eliminere sårbarheten blir også sett på. Sårbarhetene og sikkerhetstiltakene er i denne rapporten samlet for å definere et sett med sikkerhetsmetrikker som kan brukes til å kartlegge sårbarhetene i et gridsystem, måle sikkerheten, og finne hvilke sikkerhetstiltak som må gjøres for å sikre systemet.

Eksempler på hvordan metrikkene kan bli brukt til å måle sikkert er også med i rapporten. Dette for å vise at metrikkene faktisk kan bli brukt til å måle sikkerheten, og for å samle testdata. Disse testdataen blir videre brukt til å vise hvordan man kan måle avstander mellom, og klassifisere, resultatene slik at man kan ta avveninger på hvor mye sikkerhet man vil ha sammenlignet med for eksempel effektivitet..

Contents

List of Figures

List of Tables

1 Introduction

Information security is becoming an important issue in the world of today. New vulnerabilities in different systems are detected on a daily basis. Such vulnerabilities can be exploited for personal benefits, or to cause damage in an organization and its computer equipment. The need to get more of the computer resources at hand has also become more important since investing in new computer equipment can be quite expensive. One possible solution to help harvesting unused computer resources is a technology called grid computing. The essence of grid computing is joining of networks and organizations to share computational resources such as CPU time and storage. In such an environment, it would be nice to have an outline of security. The means to get an outline in such a complex environment is measuring the security in some way. A tool to measure information security are security metrics. Metrics can be used to measure security in any computing environment, but they need to be designed for the systems they are meant to measure.

1.1 Research Problem

Before continuing, it is important to define what is thought of when the expressions grid computing and grid computing environment(GCE) are used. This thesis will use the same definition as [8]. In [8], a GCE is defined in this way: A grid computing environment(GCE) is:

> A distributed computing infrastructure that supports the creation and operation of virtual organizations by providing mechanisms for controlled, cross-organizational resource sharing.

Such a grid can consist of one or more computational facilities, one or more grids, and one or more organizations. When facilities and organizations join up they form what we call a virtual organization (VO). The grid architecture is going to provide controlled mechanisms for the cross-organizational resource sharing in these virtual organizations. The main problem is that multiple architectures already exist, both security and non-security related, and different organizations tend to use different architectures. Because of this, handling interoperability becomes the main purpose of the grid architecture.

Maintaining security in such an environment is quite important, but can be a real challenge in a grid. First of all, a GCE can consist of multiple security architectures spread across different sites in the GCE. Since the interoperability is to be handled by the grid architecture, and this interoperability should be handled securely, the GCE security can be very difficult to follow. Because of this, we need some tools and routines to help us in this challenging task - making the grid secure.

The purpose of this study is to develop security metrics to measure the security in a GCE environment, and show how these metrics can be used to measure the security. This metrics will measure the level of implementation of mechanisms needed to secure a GCE. By using these metrics, an organization should be able to have an outline of the security within the GCE, and be able to isolate security related problems and in the end be able to keep the GCE secure.

1.2 Motivation

Today organizations often have a lot of unused computer resources locked up in desktop computers. Since this computational power is already in the organization, it could be tempting to implement a grid computing solution to make use of these resources. Even when just implementing such a small grid, security is a problem, since the grid could process confidential information, and most of the desktop computers are in use by ordinary employees. There is a possibility that this information needs to be encrypted. A security measurement tool such as a set of metrics may help the organization find these threats so they can be impaired or eliminated.

Some organizations have different departments at different locations. Nowadays those departments are usually interconnected using an Internet connection. An ordinary Internet connection is hardly something that can be called a trusted or secure channel. If the organization is going to expand the grid, using the Internet as the network connection, metrics will help identify threats and vulnerabilities the organization faces. If all the communication between the departments is already encrypted, the metrics will take this into account. Perhaps the needed security mechanism is already in place.

A grid is not intended to exist only within one organization. A grid can span several organizations the same way it spans different departments. When the grids span different departments and organizations, trust becomes a security factor. One may ask if sufficient trust relationships are established or if there is a need for other security mechanisms that ensure everything is secured properly.

The main benefit from security metrics is the ability to know how secure the implemented, or the soon to be implemented, grid architecture is. This makes the organization capable of identifying vulnerabilities, impairing them and enhancing security.

Security metrics provide a number of organizational and financial benefits [9]. The earlier paragraphs in this chapter show how metrics can be used to measure different aspects of information security, but metrics can also be used to isolate security problems, and collect data in order to justify security oriented investment requests [9]. Not only can one justify the investments, but by using the metrics the security investments can be targeted, to get the best value from available resources [9].

Not knowing how secure the grid is, can stop organizations from implementing grids. This may become an economical problem since there are some economic benefits from grids, such as making use of free resources just laying around on desktop computers currently being wasted. Doing this can provide 93% in up-front hardware cost savings compared to High Performance Computing Systems (HPC)[1]. With grids, organizations can cross departmental and geographical boundaries, and uniformly increase the computational capacity across the whole organization.

The operational expenses of a GCE is also 73% less, compared to HPC-Based solutions [1]. Deployment of a grid computing system could be performed in a couple of days, compared to deployment times of up to 60-90 days for an HPC-Solution [1].

1.3 Research Questions

In order to define good security metrics, one needs to know what vulnerabilities a GCE faces. This is because the reason for protecting the system needs to be known. Different security disciplines needed to secure the grid will be derived from the vulnerabilities the GCE faces. One also needs to know how to design a set of metrics, and what information needs to be extracted from the GCE vulnerabilities, in order to make the metrics a useful tool when measuring the security. If there are other security architectures similar to a GCE, information about these architectures might be used to derive what is needed in the GCE metrics. To know how to measure security is also important. For example, one may be interested in what kinds of security measures are implemented, if implementation evidence (evidence of security mechanisms being implemented) is a good way to measure the security.

Here we summarize the research questions answered in this thesis:

1. Is it possible to define a set of metrics for a GCE?
2. Is implementation evidence useful as a security measurement criterion?
3. Can the security measurement of a GCE be quantified?
4. Are security metrics based on implementation evidence useful when measuring security in a GCE?

To help answer these questions one needs to take a closer look at what has already been done in the area of grid computing security (GCS).

2 Previous work

To protect a system, one needs to know what kind of security mechanisms is needed, and why these mechanisms are needed. This can be based upon what is generally needed to make a system secure, as well as the aspects concerning the specific system at hand. If the reason for implementing a security mechanism is not known, one can ask if there is any real need for the mechanism in question. Another reason for knowing why we should implement mechanism is that a set of security metrics could be based upon this. Let us say that authentication is needed for some service on the computer network. The authentication data could be sent in plaintext over the network, but this would make the authentication data easily forgeable. If a mechanism were implemented to handle this authentication in a secure way, the authentication data could be secured in such a way that they would be almost impossible to forge. This would make the system more secure. Forgeable authentication data are a vulnerability in the system. This vulnerability can be removed by implementing a mechanism as described above. A metric could make us check if such a mechanism is implemented. If such a mechanism is not implemented we know that our system might not be secure enough. This metric is based on implementation evidence of a mechanism to remove the vulnerability. So knowledge about what vulnerabilities a grid faces is needed.

2.1 Information Security

In [11] it is defined how a system could be secured. A definition of what information security is, is also given:

> Information security is characterized here as the preservation of:
>
> 1. Confidentiality: ensuring that information is accessible only to those authorized to have access.
> 2. Integrity: safeguarding the accuracy and completeness of information and processing methods.
> 3. Availability: ensuring that authorized users have access to information associated assets when required.

Those three basic components of security are also mentioned in [3], where confidentiality is said to be concealment of information and keeping unauthorized entities from getting access to the information, where integrity refers to the trustworthiness of the data by preventing improper or unauthorized change of the data, and where availability refers to the ability to use information or resources desired.

Traditionally information security has been thought of as protecting the confidentiality and integrity in the system, but as we can see both [3] and [11] mention availability as an aspect of security. In order to explain this, we need to look at the definition of availability. Both [3] and [11] define availability as ensuring the ability to access information when required or desired. If someone deliberately arranges to deny access to data or to a service by making it unavailable, availability becomes a part of security since this should not happen in a secure system [3, 11].

The basic concepts of security are already covered, but we are now interested in how can these three basic aspects be protected. Taking a closer look at both [3] and [11] reveals that they both mention access control. In [11] access control encompasses a broad range of security mechanisms. Mechanisms mentioned in [11] are privilege management, which is a part of authorization, user authentication, node authentication, network segregation (perimeter security), encryption and integrity control. In [3], encryption, authentication and authorization (access control lists) are mentioned. Access control basically protects both confidentiality and integrity since access control keeps unauthorized entities away from the information such that they cannot access or change it.

[23] looks at services and mechanisms to protect the security, and takes a closer look at some of the standards and technologies. Security services mentioned in [23] are: authentication, access control, non-repudiation and availability. In [23] authentication is defined as the assurance that the entity communicating is the one that it claims to be. Authentication also encompasses data-origin authentication, which assures that the source of the received data is as claimed. The access control mechanism in [23] includes data confidentiality and data integrity.

As for now, the confidentiality and integrity part of information security is covered, but protecting the availability is hardly mentioned. In both [3] and [23] , the need to detect and/or stop a denial of service attack is mentioned, but other than that it is difficult to define mechanisms to prevent this. [23] sees the need for network transmission protocols to be robust and withstand a denial of service attack.

2.2 Similar Environments

In general a GCE is an ordinary computer network, but what separates a GCE from other networks is the special kind of resource sharing requirement [8]. A GCE is actually a form of distributed computing [16]. Due to this a GCE faces the challenges that all ordinary networks face [23], in addition to those brought forward because of the resource sharing is needed. One of the challenges an ordinary network faces, which also holds for a GCE, is network perimeter security [24].

When employees of a company need to access internal resources from outside of the network perimeter, a virtual private network (VPN) is often set up to handle this [17, 24]. This is quite similar to different networks joining into one virtual network and sharing their resources.

A network infrastructure quite similar to the GCE in general is the Web Services (WS) architecture, which has its own security architecture, the Web Services Security architecture (WS security) [8, 18]. The WS security architecture has already defined some structures, which may be used for GCE security, such as security token/credential profiles used for exchanging credentials between different different security architectures [4-6,9,21]. The WS security architecture has also defined a way of forwarding security privileges using soap [4, 5].

2.3 Grid Vulnerabilities

Most of the vulnerabilities come from what was stated in the definition of a grid - virtual organizations (VOs) [8, 27]. VOs require the establishment of trust and associated security across multiple organizational boundaries [8].

A vulnerability that is present as a consequence of belonging to the VOs, is the fact that a grid will span multiple security architectures [8, 27]. The vulnerability in this case is the interaction between the grid and the security architectures. This interaction has to be defined in a clean and secure way.

In a GCE services (e.g. "resources") are created dynamically. If these resources are not coordinated and handled securely, vulnerabilities arise. In such an environment the VOs are also expected to join and leave the grid infrastructure dynamically [8, 27]. This will also bring forward vulnerabilities if not coordinated or handled securely.

Since messages can be transmitted from one VO to another on its way to the VO they are destined for [8], some vulnerabilities may emerge. One may have to decide whether the grid system should rely on the transport layer to ensure confidentiality and/or integrity of the information, or if this should be done at the message-layer. Transport layer encryption is often based on node to node encryption. If the grid relies on the transport layer to perform the encryption, vulnerabilities arise at nodes that decrypt the messages. This is because at such a node confidentiality will be broken for at least a short period of time, and integrity checks will most likely be removed.

Since the grid spans different organizations and different security architectures, they also span different security policies. The grid needs to exchange these policies in order to establish a negotiated security context between services [8]. If these transactions are not coordinated or handled securely, the systems will be vulnerable. Fake security policies could be inserted, or modifications could be done to the policies that are already in a transaction.

Another vulnerability that arises from messages transmitted between different VOs, is concerning authentication. If there is a particular message coming through, and we recieve it from a VO with little trust, but we do trust the VO that sent it, we do not know for sure if the real sender is the one claimed by the message. Here an authentication schema is needed, to open for message authentication. This should most likely be joined with integrity mechanisms, since if the message integrity is lost one cannot really trust any of the message contents.

2.4 Grid security disciplines

Besides knowing what vulnerabilities the system faces, knowing which security mechanisms are needed in order to impair the vulnerabilities is valuable information, when making a system secure. In [11], information security is defined to be protecting the confidentiality, integrity, and availability of the information, services and the systems included in the system to be protected. Hence we need mechanisms to protect these 3 attributes of security. This section is devoted to looking at various mechanisms needed to handle the security within a GCE. The mechanisms listed here are based on the list that can be found in [8] and [25]. In [25], even a first draft of a policy for a GCE is listed.

2.4.1 Authentication

Authentication is usually linked close together with authorization. Authentication and authorization are often used in a combination in order to grant someone access to a service or a resource based upon a given identity. In both [8] and [25], authentication is pointed out as a distinct mechanism with the purpose of verifying proof of an asserted identity. The authentication mechanism in a GCE is to provide plug points for the multiple authentication mechanism at hand, and the means for conveying the specific mechanism used in the authentication operation. In [7], it is stated that in order to get a strong authentication mechanism single sign-on is needed. This is because multiple authentication requests are bothersome and will likely be circumvented if possible. Web services security (WSS) [18] is a security structure designed for systems similar to a GCE. In WSS mechanisms that may be used for authentication in a GCE are already implemented, such as Public Key Infrastructure [6, 22]

2.4.2 Single sign-on

Single sign-on is needed because participants in a GCE often need to coordinate multiple resources just to solve one single task. Manually performing an authentication process in such a scenario would be overly burdensome. A security mechanism is needed to ensure that an entity having successfully completed the act of authentication once, won't need to re-authenticate in a given period of time. One must remember that requests may span several security domains and should hence be a factor between authentication domains and mapping of identities. Because of this, delegation of an entitys rights and the ability to indicate the identity of intermediate entities is needed.

2.4.3 Credential life span and renewal

Credentials have to be renewed after a given period of time. This is to limit the risk of compromise in delegation and single sign-on [8, 13, 26]. Different tasks in the GCE will have different lifespan and execution time. Execution time for performing the same task can vary because of resource usage from other services in the grid. Because of this, it will not always be possible to predict the precise credential lifetime needed for a task. A user needs to be notified or have the possibility to refresh his credentials if a task takes longer time than the lifetime of his initial credentials.

2.4.4 Authorization

Authentication is usually closely linked to authentication (e.g. authentication is needed to access services, which the entity is authorized to use). To access specific services in the grid, one needs to be authorized to access that service first. In a grid, authorization policies work both ways (not only as in the basic model where policies are being specified by the resource owner). This is because requestors may need the provider to fulfill some requirements. Policies for authorization should also mention if mutual authentication is needed [19].

2.4.5 Delegation

The VOs in a grid underlying collaborative work, may form quickly, evolve over time and span organizations [8]. The effective operation of these VOs depends critically on trust. One solution to this is establishment of dynamic trust domains where one entity can assign rights to another. To manage this, a delegation service is needed such that authority can be delegated from one entity to another. This delegation should work by the 'least privilege model [21]' and be scoped for a limited time to minimize misuse. Delegation is also needed to secure dynamic service creation [8, 10]. This mechanism/discipline is also recognized in [28].

2.4.6 Privacy

Both service requestor and provider must be allowed to define and enforce privacy policies, taking into account personally identifiable information for the purpose of invocation. In [8] it is stated that privacy policies may be treated as an aspect of authorization policy addressing privacy semantics such as information usage rather than plain information access.

2.4.7 Confidentiality

Both the underlying communication mechanism and the messages or documents flowing over this given transport mechanism should preferably be confidentiality protected. If only the transport mechanism were protected, the information might be unprotected for a short time while on transportation endpoints in the grid. If the message has to go through a computational facility, the transport layer will probably decrypt it, and then encrypt another time before the message is forwarded. Because of this message encryption is also needed. This means that confidentiality requirements includes point to point transport as well as store and forward mechanisms. The need for communication security such as confidentiality is also pointed out by [10, 19, 26].

2.4.8 Message integrity

Both confidentiality and non-confidentiality protected information can be altered. To protect against unauthorized changing of information in messages/documents some kind of integrity protection is needed. Preferably the transport mechanism should at least have integrity protection that guards against transmission errors, but also against intended but unauthorized altering of the information. Using integrity and confidentiality protection can help in achieving communication security [10, 19, 26]. Using integrity protection at the message/document level is often subject to policy and quality of service requirements.

2.4.9 Policy exchange

As mentioned in the authorization section, authorization policies have to work both ways. Because of this, authorization policies need to be dynamically exchanged. Another reason for exchanging security policies is the need to establish and negotiate security contexts. The following policy information can be exchanged: authentication requirements, supported functionality, constraint and privacy rules. This exchanging of policies, both security related and non-security related, should preferably be performed in a secure manner.

2.4.10 Secure logging

Logging is important to make a foundation for addressing requirements for notarization, non-repudiation, and auditing. This logging should be performed in a secure manner, or else this logging can't be trusted. Logging should include secure logging of any kind of operational information or event since this can be used for auditing. Logging in a secure manner means reliably and accurately, which means so that such logging is neither interruptible nor alterable by an adversary.

2.4.11 Assurance

Means to qualify for the security level expected of a hosting environment, must be provided by every participating node. This includes what security measures and mechanisms are implemented, and a policy of their usage. This can be virus protection, firewall usage for internet access, and internal virtual private network usage [17, 24].

2.4.12 Manageability

The ability to manage security in a grid is needed. The fact that a grid needs authentication and authorization indicates that both identity and policy management are needed. This management also includes higher-level requirements such as virus protection, intrusion detection and prevention. Virus protection and intrusion detection are requirements on their own, but are typically provided as part of security management.

2.4.13 Firewall traversal

First of all, firewalls are major barriers to dynamic and cross domain computing in general, and also to cross domain grid computing [2]. Firewalls might only be of minimal value in an environment that carries out dynamic cross-domain computing, but firewalls are unlikely to disappear anytime soon [8]. Because of this, a grid must take firewalls into account so that they can be traversed securely without compromising local control of firewall policy.

2.5 Security Metrics

2.5.1 Definition of grid security requirements

The grid security disciplines listed by [8] and [26] seem to be a good start for setting requirements that must be fulfilled to get a secure system. Those security disciplines seem to be what the literature mentions as needed for a grid computing system.

2.5.2 A possibility of defining a set of metrics for a GCE

As it can be seen from Chapter 2.2, there is a lot of information on grid security requirements, and as mentioned in Chapter 2.2, a security policy for GCEs is defined in [25]. A metric should be based on security requirements and policies. After all, requirements and policies are what defines the needed security. So the criteria needed to measure the security seem to be available.

Security metrics do not seem to be the most developed area of research, but still there are some sources available with information on how to create metrics. In [9], a thoroughfare on metrics development and implementation approaches is presented.

According to [9] , the metrics development process within a larger organizational context consists of these 7 phases (Figure 1):

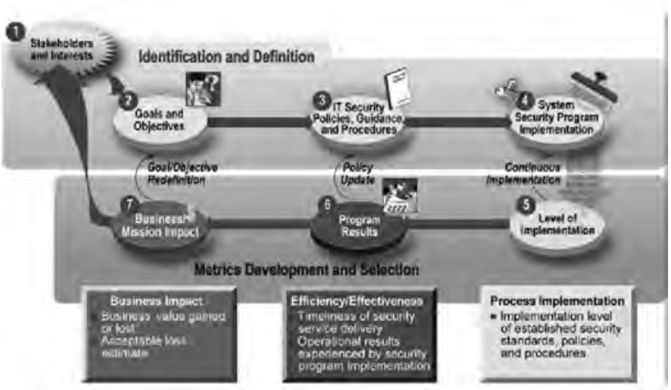
1 Stakeholders and Interests
Identification and Definition
2 Goals and Objectives
3 IT Security Policies, Guidance, and Procedures
4 System Security Program Implementation
Goal/Objective Redefinition
Policy Update
Continuous Implementation
7 Business/Mission Impact
6 Program Results
5 Level of Implementation
Metrics Development and Selection
Business Impact
Business value gained or lost
Acceptable loss estimate
Efficiency/Effectiveness
Timeliness of security service delivery
Operational results experienced by security program implementation
Process Implementation
Implementation level of established security standards, policies, and procedures

Figure 1: Metric development process

1. Stakeholders and Interests
   Identify the primary IT security stakeholders.
2. Goals and objectives
   Identify and document system security performance goals, and objectives that would guide security control implementation for that system.
3. IT Security Policies, Guidance and Procedures
   Look at documentation on currently implemented security measures, so that one can concentrate on metrics for controls not yet implemented.
4. System Security Program Implementation
   Review applicable information needed to derive security metrics data.
5. Level of Implementation
   The three last phases in the developing of metrics are related to process implementation, effectiveness and effiency, and mission impact.
6. Program Result
   Effectiveness and effiency.
7. Business Mission Impact
   Mission Impact.

According to [9] the IT security metrics development consists of two major activities:

1. Identification and definition of the current IT security program; and
2. Development and selection of specific metrics to measure implementation, efficiency, effectiveness, and the impact of the security controls.

Examples of previous implementations of security metrics can be found in [14], which focuses on finding performance indicators and developing security metrics for perimeter security. In [20], there are examples of indicators and metrics that can be used for measuring robustness in password protection. Examples on different metrics can also be found in [9].

2.6 Metric data examination

As mentioned in [9], metrics can be used to prove the value of implementing a security measure, by showing how much better the security gets when implementing this measure. From the results of the evaluation of the security metrics, one might see if it is worth implementing a security measure from an economical point of view. When securing the system one might be aiming for an ideal point, such as 100% security. So when looking at the results of the security metrics one may want to know how far from the ideal point the measurement is.

When measuring security, one often ends up with vectors describing the security. This is especially true if one is using metrics where the result of each metric is a coordinate of the vector describing the security configuration in question. To measure the distance, one could use metrics for analyzing vectors as described in [15]. One way of measuring the distance mentioned in [15] is the Euclidean distance (L2 metric). To analyze how good a security configuration is, one can measure the distance from the ideal point using this euclidian distance which is calculated in the following way:

$\mathrm{Eucl}(\mathbf{X},\mathbf{Y}) = \sqrt{\sum_{i=1}^{d}(x_i - y_i)^2}$

This formula calculates the distance between the d-dimensional vector **X** and **Y** where x_i and y_i denote coordinates of the respective vectors.

It is not always possible to define an ideal point. This is because one might want both optimal speed, and optimal security, which not always works together. Availability is often thought of as an aspect of security [3, 11]. In [23], different extensions of availability are presented. The time to access information can be thought of as one aspect of availability, and when the mean time to access the information increases, the availability is reduced. Putting in different security measures such as encryption can reduce the availability by increasing the mean time to access the information. When this happens it is difficult to define an ideal point since increasing one aspect of security would reduce another aspect of security. In such a case one could classify the measurement vectors by putting them into clusters with similar vectors. Algorithms to put these vectors into clusters are described in [12]. Using clusters requires several measurements over time where the security configuration is changed in between each measurement, in order to get vectors to fill the clusters.

One algorithm that may be adequate for classification necessary in this thesis is the k-means algorithm described in [12]. The following is an outline of how this algorithm works, and will be used in this thesis:

1. First, k vectors are chosen at random, to be used as centers of the clusters.
2. Now each measurement is assigned to the closest cluster center (can be done by calculating the euclidean distance from the centers)
3. Recompute the cluster centers as the mean of the current cluster members.
4. If the convergence criterion is not met, goto step 2. The convergence criterion could be: No or minimal reassignment of vectors to new clusters when the new centers are calculated.

3 GCE Metrics

In this chapter a set of indicators that could be used in security metrics for grid computing environments is addressed. The focus is on metrics that check if security measures actually are implemented where needed to make grid communications and usage secure. Each metric measures percentage of implementation level, thus giving a number in the range 0-100%. Having a score of 100% on one particular metric does not necessarily imply 100% security, but tells that the security measure is implemented 100%. Similarly, a total score of 100% from all the metrics does not mean that the system is 100% secure, but that security measures checked in the metric are at the implementation level of 100%. The metric development focuses on phase 4 and 5 in Fig1, Chapter 2. In Chapter 4, the focus is on the phase 4, and in Chapter 5 the focus is on the phase 5.

3.1 Metric Definition

These metrics are supposed to measure security based on the security definition given in [11]. Looking at Chapter 2, Section 1, 2 and 3 leads to the need of measuring access control and transaction confidentiality to measure confidentiality, and access control and transaction integrity to measure the integrity. Access control is based on two basic measures, authentication and authorization, which are measured in separate metrics. A separate metric is defined for availability. This results in 6 separate metrics:

1. Authentication,
2. Authorization,
3. Transaction confidentiality,
4. Transaction integrity,
5. Perimeter security and
6. Availability.

To make sure the measurements from the different metrics are comparable, the metrics are based on the following metric template (based on the template found in [9]):

Table 1: Metric template

Name	Descriptive name of the metric. Such as: Authentication
Performance Objective	State the actions that are required to reach the performance goal
Implementation evidence	A list of questions to give an outline of the implementation level of this particular security mechanism.
Frequency	Propose time periods for collection of data that is used for measuring changes over time.

Formula	A description of the formula and numbers used to calculate a result based on the different answers from the Implementation Evidence section of the metric. This calculation must result in a number that makes all the metrics comparable, making it easier to understand the results. For the metrics used in this paper, ratios are used as the measurement. The result of the formula must end up as a number in the range: 0-1 ((0-100)%). This indicates the level of implementation of the security mechanism in question.
Indicators	A short narrative on the purpose of the metric, what this metric measures and indicators the Implementation Evidence section will use as questions.
Cost	The cost of using this metric to measure a system. The cost is measured in hours.

3.1.1 Authentication

Authentication is a part of access control, used to protect both confidentiality and integrity in information security. This metric measures the implementation level of the authentication mechanism in the GCE.

Table 2: Authentication metric

Name	Authentication
Performance Objective	Make sure participants of the grid are authenticated properly (verify proof of asserted identity).
Implementation evidence	Q1. What is the number of nodes requiring authentication to get access? Authentication on direct connections or local users. The number of nodes with proper authentication schemes should be the answer to this question. Q2. What is the number of nodes requiring end-to-end authentication? Authentication of source/destination nodes. The total number of nodes with end-to-end authentication support should be the answer for this question. Q3. What is the highest number of authentications needed to access more than one service? If the user needs to perform one authentication procedure only, single sign on is implemented. The total number of authentication procedures needed, to accomplish one task that needs to use more than one resource in the grid is the answer for this question.
Formula	$f(x) = \frac{(\frac{q1}{totalnumberofnodes} + \frac{q2}{totalnumberofnodes} + \frac{1}{q3})}{2}$ Calculates the implementation level at each question, and calculates the average implementation level of this metric.

Indicators	Authentication is a part of the access control in a system. If entities do not need to tell what or who they are when accessing a system, it indicates that anyone could access the resources and services in that system. If the system stores information that needs to be confidential and entities accessing these resources do not need to identify, this indicates poor security and access control. Any entity can claim to be someone else. If this identity claim is not verified, anyone can still access the resources by giving false credentials to the system. If there are nodes in the network not requiring authentication, this may be a weak spot where people may gain access to the grid unauthenticated. If there is a policy on a node in the grid, saying that entities accessing this node can be verified by this node only, we might need more than just simple authentication. Since messages can be transmitted from node to node, someone who cannot be verified by the particular node might send the message trough a node that can be verified at the particular node, and in this way circumventing the need to authenticate. If nodes not only need to authenticate for the first node in the message path, but also to the final destination, gaining access by node skipping gets harder. Missing such end-to-end authentication indicates a possibility to breach security by taking advantage of node skipping. If users have to authenticate more than once to complete a task in the grid, they might think this is annoying and start to circumvent the authentication, one way or another. They might start to choose easy passwords, or even look for other ways to perform the authentication procedures. More than one authentication procedure does not necessarily indicate poor security, but it indicates a risk that someone, some way or another might decrease security to gain usability.
Actions	If nodes lack authentication mechanisms, such mechanisms should be implemented at these nodes. If this is not possible, one might consider denying access to the grid for these nodes. Nodes lacking end-to-end authentication mechanisms that can communicate with the rest of the grid should not host any high-security grid-resources. If high-security communication with these nodes is needed, end-to-end authentication mechanisms at these nodes are also needed.

3.1.2 Authorization

Authorization is a part of access control which is usually closely related to the authentication and is used to help ensure the confidentiality and integrity in Information security. This metric measures the implementation-level of authorization mechanisms in the grid.

Table 3: Authorization metric

Name	Authorization

Implementation evidence	Q1. What is the number of nodes requiring authorization to get access? Checks the level of implementation of ordinary authorization(local users) The answer to this question should be the the total number of nodes with this mechanism. Q2. What is the number of nodes requiring end-to-end authorization? Checks the level of implementation on end-to-end authorization. The answer to this question should be the the total number of nodes with an end-to-end authorization scheme.
Formula	$f(x) = \frac{(\frac{q1}{totalnumberofnodes} + \frac{q2}{totalnumberofnodes})}{2}$ Calculates the implementation level of both ordinary authorization and end-to-end authorization. Finally, the formula calculates the average of these two and uses this as the final result of this metric.
Indicators	One aspect of access control is authenticating entities, but knowing the identity of an entity may not be enough. If all authenticated users got access to everything, they might get access to resources they do not need or should not have access to. Access control missing some kind of authorization scheme indicates that people can gain access to resources they should not. The authorization part of access control is just as vulnerable for messages being transmitted from node to node as the authentication part is. If some entity which is not authorized to use a specific service, manages to get access, by letting an authorized entity access it on its behalf, there is most likely a security breach.
Actions	Implement a centralized authorization policy, which defines a basic authorization scheme every node needs to comply with. Implement a system where authorization is based on the credentials given in the end-to-end authentication scheme.

3.1.3 Transaction confidentiality

Even with proper access control based on authentication and authorization mechanisms, confidentiality might be at risk in a distributed system. This is if the confidentiality of the communication is not protected. Encryption of data or communication lines can be looked at as a part of access control. This is because the proper key is needed to decrypt the information. This metric measures the implementation-level of encryption/transaction-confidentiality.

Table 4: Transaction confidentiality metric

Name	Transaction confidentiality
Performance Objective	Ensure confidentiality

Implementation evidence	Q1. How many communication lines have confidentiality protection? Checks for network connections with confidentiality protection such as a VPN. The answer to this question should be the total number of communication lines with confidentiality protection. Q2. How many nodes require end-to-end message encryption? Checks the implementation level of end-to-end message confidentiality based on cryptography. The answer to this question should be the total number of nodes nodes requiring messages are end-to-end encrypted.
Formula	$f(x) = \frac{(\frac{q1}{totalnumberofcommunicationlines} + \frac{q2}{totalnumberofnodes})}{2}$ calculates the implementation level of both communication lines security and end-to-end encryption, and uses the average as the score for this metric.
Indicators	Transaction confidentiality can be based on at least two different schemes. These are message confidentiality and communication line confidentiality. If we consider a scenario with only message level encryption, an intruder could make the systems not encrypt the messages sent. In such a way, someone could gain access to the information being communicated through tapping the communication line. When looking at confidentiality this way, unencrypted communication lines indicate a security weakness. When encrypting at the communication level, one can argue that message encryption is not needed, since the communication line is already encrypted and people tapping this line will only get something that looks like random data anyway. The problem appears when a message is transmitted from node to node on its way to the destination. If only the communication lines are encrypted, the message will most likely be decrypted and encrypted at the intermediate nodes, leaving the message unencrypted for a short period of time. If an adversary has gained access to one of the intermediate nodes, the adversary only needs to monitor the network flow on the compromised computer in order to gain access to information sent trough that node. Having this in mind, missing source to destination (end-to-end) encryption might indicate a security flaw.
Actions	To secure the communication lines, some kind of VPN could be implemented to encrypt the communication lines. End-to-end encryption is often application dependent, thus software that accesses grid services should be enhanced with end-to-end encryption capabilities.

3.1.4 Transaction integrity

Ordinary access control and confidentiality protection (encryption) is not enough to secure a line properly. A determined adversary could still be able to change the data transmitted, and by doing this compromise the integrity of our GCE. This metric measures the implementation level of integrity protection mechanisms needed by the grid.

Table 5: Transaction integrity metric

Name	Transaction integrity
Performance Objective	Ensure the integrity of the communication lines and messages sent over these lines
Implementation evidence	Q1. How many communication lines have integrity protection? Checks the implementation level of integrity protection on the communication-lines. This integrity protection should be cryptographic integrity protection, e.g. as offered by a VPN. The answer to this question should be the total number of communication-lines with satisfactory message integrity protection. Q2. How many nodes require end-to-end message integrity encryption? Checks the implementation level of end-to-end message integrity. This integrity protection should be some kind of cryptographic integrity protection, such as cryptographic message digests and/or cryptographic signatures.
Formula	$f(x) = \frac{(\frac{q1}{\#lines} + \frac{q2}{\#nodes})}{2}$ Calculates the implementation level of each of the indicators in the implementation evidence section and uses the average as the score for this metric.
Indicators	Communication integrity can be based on both communication line integrity and message integrity. A scenario where one uses end-to-end message integrity might be compromised if someone makes the systems send messages with no integrity protection. The absence of communication line integrity protection might indicate a security flaw which can be used to make unauthorized and undetectable changes to information being transmitted. If there is integrity protection on the communication lines only (no end-to-end integrity protection), messages can, for a short time, exist on intermediate nodes without integrity protection (e.g. if a message needs to visit one or more nodes on its way to the destination node). On these intermediate nodes, some adversary might have gained access and can change the information, before it is retransmitted to its final destination.

Actions	Most VPNs come with both confidentiality protection and integrity protection. Setting up VPN connections can protect both the confidentiality and the integrity of the communication line. To achieve end-to-end message integrity one could attach a signature to the message. Some sort of a hash-funtion may also be used.

3.1.5 Perimeter security

If an adversary manages to gain access to one of the nodes, he/she might manage to compromise the whole grid. This is because the adversary may compromise an account with the access to high-level security grid resources. This metric measures the implementation level of basic perimeter security.

Table 6: Perimeter security metric

Name	Perimeter security
Performance Objective	Ensure viruses and spam do not propagate through the network, and that unwanted entities cannot break into the system.
Implementation evidence	Q1. What is the number of non-GCE specific communication lines with proper intrusion prevention systems? The answer to this question is the total number of other connections with intrusion prevention systems (IPS). Q2. What is the number of non-GCE specific communication lines with proper intrusion detection systems? The answer to this question is the total number of other connections with intrusion detection systems (IDS). Q3. How many nodes in the GCE are properly virus protected? The answer to this question is the total number of nodes with proper virus protetction. Q4. How many nodes in the GCE are properly protected against spam? The answer to this question is the total number of nodes with proper spam protection. Q5. What is the number of internal GCE network-connections with a proper IPS? The total number of GCE internal connections with IPS is the answer to this question. Q6. What is the number of internal GCE network-connections with a proper IDS? Checks for implementation evidence of IDS on GCE internal network connections. The total number of GCE internal connections with IDS is the answer to this question.

Formula	$f(x) = \frac{(\frac{q1}{\#ngcelines} + \frac{q1}{\#ngcelines} + \frac{q3}{\#nodes} + \frac{q4}{\#nodes} + \frac{q5}{\#gcel} + \frac{q6}{\#gcel})}{6}$ Calculates implementation level of each of the indicators in the implementation evidence section and uses the average as the score for this metric.
Indicators	In a GCE there can be many network connections, both physical and logical. Most of the network connections would be GCE internal connections (the connections between nodes in the grid), but some connections can be to other networks such as the Internet. The grid can be looked at as a trusted zone, and we want to keep unwanted entities away. If connections to other networks are not properly protected (with IDS and IPS), there is a possibility that unwanted entities can gain access to the grid (i.e. no IDS/IPS indicates the network is not secure enough). If unwanted entities gain access to a node in the GCE we should have some kind of damage control, keeping the security breach at one node. IPS and IDS on all network connections could help confine the security-breach to the node where it initially took place. Spam and viruses are annoying features of most computer networks connected to external networks (networks one cannot control, such as the Internet). A grid without spam protection can easily be flooded, and nodes connected to external networks should have proper spam protection to keep spam from entering the grid. Nodes missing spam protection indicate that spam can propagate trough those nodes if it manages to enter the GCE. Viruses can also be spread by e-mail, and spam filters could probably stop some of them. Viruses can get into the GCE from external network connections, but also from laptops, handheld devices and portable storage equipment. Viruses can open backdoors into the systems, and nodes without proper virus protection could indicate security being jeopardized.
Actions	Lower score on any of the questions in the implementation evidence section indicates that one or more nodes are missing the security mechanism in question. To get better security, firewalls, intrusion detection systems, and virus and spam protection needs to be implemented.

3.1.6 Availability

This metric measures implementation evidence of mechanisms that try to prevent the loss of availability. One can look at availability as the ability to access a service in a timely manner. This metric, however, does not look at that aspect of availability, but this is measured as efficiency when these metrics are tested.

Table 7: Availability metric

Name	Availability
Performance Objective	Ensure entities and services can access other entities and services in the grid.

Implementation evidence	Q1. For each node: Total number of direct connections to other nodes. Checks for implementation evidence of direct network connections to other nodes in the network. This question should have as many answers as there are nodes. Each of these answers should be the total of other nodes this node has a direct connection to. Q2. For each service: Number of nodes with this service. Checks for implementation evidence of service redundancy. This question should have as many answers as there are grid-specific services. For each of these services, the answer should be the total number of nodes that host this service.
Formula	$\frac{(\frac{\sum_{n=1}^{\#nodes}\frac{(node(n)\ connections)}{\#nodes-1}}{\#nodes})+(\frac{\sum_{n=1}^{\#services}\frac{\#ofNodesWithService}{\#nodes}}{\#services})}{2}$ This calculation is slightly more advanced than those for the rest of the metrics, since both questions have multiple answers. To calculate the implementation level for Q1, we need to take the sum of all the answers from Q1, where each answer is divided by total number of nodes minus 1. Then we divide the sum by the total number of nodes. To get the level of implementation in Q2 we need to take the sum of each answer from Q2, where each answer is divided by the total number of nodes. Then we divide the sum by the total number of services. To get the score for the metric the average score is taken.
Indicators	If there is one central node which all other nodes connect to, and all the other nodes are connected to this one only, noone can communicate if some adversary manages to bring down the central node. The more nodes each single node is directly
Indicators	connected to, the more nodes are needed to be disabled to stop users from gaining access to the services and resources they need. A small number of connections in a grid might indicate that availability might be breached if a certain number of nodes is brought down by an adversary. The availability of services and resources is not only a function of how large the number of paths between nodes is. If a service or resource only exists on one node, this node is the only one that needs to be brought down in order to remove the availability of this particular service. Low service/resource redundancy might indicate this service being vulnerable to an availability attack.
Actions	One can increase the number of direct connections to other nodes, or one could try to set up different services in the grid to run on as many servers as possible.

4 Measurements

This chapter focuses on phase 5 of the grid development cycle. In this chapter, the metrics are tested to show how they can be used to measure the security in a GCE. Besides, the efficiency of the grid is measured with different security configurations. To carry out this, a small local network is used.

4.1 GCE Base configuration

The base network that is used for all the tests in this report consist of 5 ordinary desktop computers with fedora core 1 as the operating system(OS). The hardware varies from from 233MHz to 1,7GHz computers. To get a grid computing environment, the Globus Toolkit version 3 [8] is used. The Globus Toolkit uses PKI504 certificates for authentication [27]. The hosts in the network are equipped with gridFTP servers using the gsiftp protocol to transfer information. Each computer has secure shell (SSH) server and client installed by default. This results in SSH being the choice for setting up a VPN.

4.2 Measurement procedure

To answer the questions in the metrics, a look at the configuration of the grid is needed to sort out which security measures are actually implemented in the GCE. In a real world example this can be done by reading documentation, looking at configuration files and testing the grid to see if it actually is as secure as the documentation/configuration files say. The efficiency of a security configuration is measured by using gridFTP to transfer files from host to client, where the client is the requester and the host is the responder. To get an average time for one specific transfer, a simple php script transfers a 25866130 byte tar gz compressed file 25 times, and calculates average time. Effectiveness is measured in bytes transfered per second. To carry out the measurements, and to answer the questions in the metrics, the most secure setting is tested first. Then parts of security mechanisms get removed one by one to get other configurations. The result of each measurement is a vector with 6 coordinates. These coordinates are the result from each of the metrics. The coordinates are in the same order as the metrics are defined in Chapter 3. The metrics are not included when measuring. A table that includes all the questions, the score calculations, and the total metric score is used instead.

4.3 Ideal configuration

Before the measurements start, an ideal point should be defined. The ideal point is the most secure configuration (all scores 100%). This results in the following values of the metric:

Table 8: Ideal configuration

Authentication	Q1	100%	100%
	Q2	100%	
	Q3	100%	

Authorization	Q1	100%	100%
	Q2	100%	
Transaction confidentiality	Q1	100%	100%
	Q2	100%	
Transaction integrity	Q1	100%	100%
	Q2	100%	
Perimeter security	Q1	100%	100%
	Q2	100%	
	Q3	100%	
	Q4	100%	
	Q5	100%	
	Q6	100%	
Availability	Q1	100%	100%
	Q2	100%	

The ideal point vector can be taken directly from the rightmost column:

$idealp = (100, 100, 100, 100, 100, 100)$

Ideal point with efficiency:

$idealpe = (100, 100, 100, 100, 100, 100, 100)$

Where the last one is efficiency measured in percent.

4.4 Network 1 - Measurements

The first network consists of 5 nodes, where each node is connected to every other node in the network. These connections are not physical connections but virtual connections set up by using SSH. Each of the nodes has its personal firewall (ip-tables), where the only open port, besides the ones configured during the basic fedora installation, is the port 22. The network topography of network 1 is shown in Figure 2.

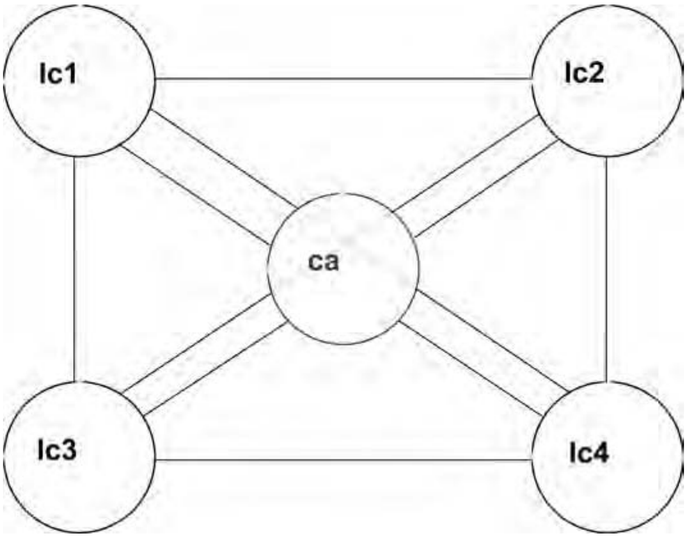

Figure 2: Network 1

4.4.1 Configuration 1

In this first configuration, gridFTP with full protection (both integrity and confidentiality) is used. This network has no external network connections, and the only perimeter security mechanism is the ip-tables firewall, which is in this case considered a proper IPS.

In this first measurement I will include the table and a figure (Figure 4.4.1) showing the security configuration. In the later measurements only the figure will be included, and the tables can be found in appendix A.

Table 9: Measurement n1c1

Authentication	Q1	$\frac{5}{5} = 100\%$	$\frac{Q1+Q2+Q3}{3} = 100\%$
	Q2	$\frac{5}{5} = 100\%$	
	Q3	$\frac{1}{1} = 100\%$	
Authorization	Q1	$\frac{5}{5} = 100\%$	$\frac{Q1+Q2}{2} = 100\%$
	Q2	$\frac{5}{5} = 100\%$	
Transaction confidentiality	Q1	$\frac{10}{10} = 100\%$	$\frac{Q1+Q2}{2} = 100\%$
	Q2	$\frac{5}{5} = 100\%$	
Transaction integrity	Q1	$\frac{10}{10} = 100\%$	$\frac{Q1+Q2}{2} = 100\%$
	Q2	$\frac{5}{5} = 100\%$	
Perimeter security	Q1	$\frac{0}{0} = 100\%$	$\frac{Q1+Q2+Q3+Q4+Q5+Q6}{6} = 50\%$
	Q2	$\frac{0}{0} = 100\%$	
	Q3	$\frac{0}{5} = 0\%$	
	Q4	$\frac{0}{5} = 0\%$	
	Q5	$\frac{10}{10} = 100\%$	
	Q6	$\frac{0}{10} = 0\%$	
Availability	Q1	$\frac{\sum_{n=1}^{5} \frac{(node(n)\ connections)}{4}}{5} = 100\%$	$\frac{Q1+Q2}{2} = 80\%$
	Q2	$\frac{\sum_{n=1}^{1} \frac{3}{5}}{\#1} = 60\%$	

Transfering between lcl1 and ca: Average transfer-rate: $\frac{25866130}{34,4} = 751,92KB/sec$
Transfering between lcl1 and lcl4: Average transfer-rate: $\frac{25866130}{9,6} = 2694,54KB/sec$
Average transfer-rate: $\frac{751,92+2694,54}{2} = 1723,23KB/sec$

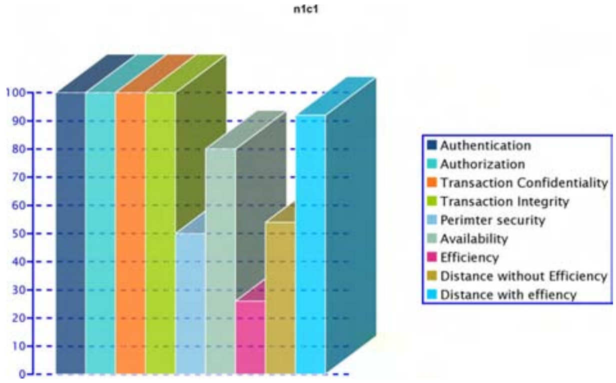

Figure 3: Network 1, measurement 1

Vectors:
$n1c1 = (100, 100, 100, 100, 50, 80)$
$n1c1e = (100, 100, 100, 100, 50, 80, 1723)$

4.4.2 Configuration 2

Basically using configuration 1, but removing end-to-end message privacy protection (encryption) from all communication lines, gives the following security profile (Figure 4.4.2):

Transfering between lcl1 and ca: Average transfer-rate: $\frac{25866130}{21,6} = 1197,50KB/sec$
Transfering between lcl1 and lcl4: Average transfer-rate: $\frac{25866130}{7,6} = 3403,44KB/sec$
Average transfer-rate: $\frac{1197,50+3403,44}{2} = 2300,47KB/sec$

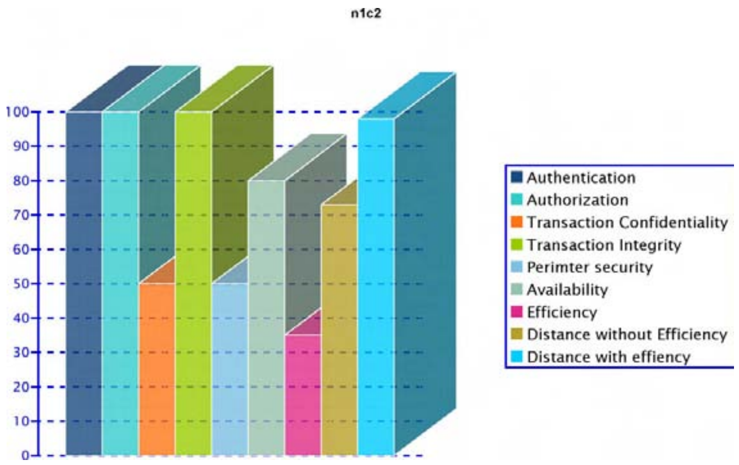

Figure 4: Network 1, measurement 2

Vectors:
$n1c2 = (100, 100, 50, 100, 50, 80)$
$n1c2e = (100, 100, 50, 100, 50, 80, 2300)$

4.4.3 Configuration 3

Keeping configuration 2, but removing the end-to-end message integrity protection from all communication lines, gives the following security profile (Figure 4.4.3):

Transfering between lcl1 and ca: Average transfer-rate: $\frac{25866130}{15,4} = 1679,62KB/sec$
Transfering between lcl1 and lcl4: Average transfer-rate: $\frac{25866130}{5,3} = 4880,40KB/sec$
Average transfer-rate: $\frac{1679,62+4880,40}{2} = 3280,01KB/sec$
Vectors:
$n1c3 = (100, 100, 50, 50, 50, 80)$
$n1c3e = (100, 100, 50, 50, 50, 80, 3280)$

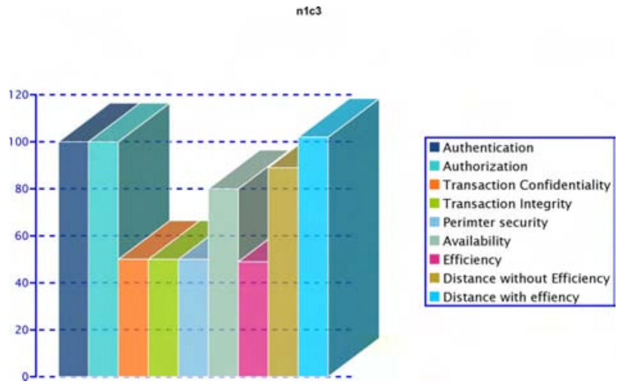

Figure 5: Network 1, measurement 3

4.4.4 Configuration 4

Reverting to configuration 1, but with the communication line security switched off (encryption), we obtain the following security profile (Figure 4.4.4):

Transfering between lcl1 and ca: Average transfer-rate: $\frac{25866130}{23,7} = 1091,40KB/sec$
Transfering between lcl1 and lcl4: Average transfer-rate: $\frac{25866130}{9,1} = 2842,43KB/sec$
Average transfer-rate: $\frac{1091,40+2842,43}{2} = 1966,92KB/sec$

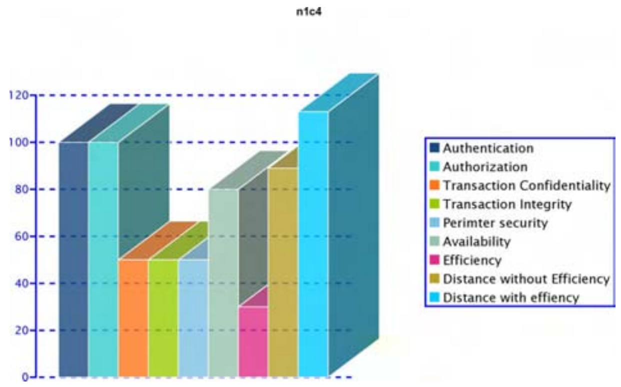

Figure 6: Network 1, measurement 4

Vectors:
$n1c4 = (100, 100, 50, 50, 50, 80)$
$n1c4e = (100, 100, 50, 50, 50, 80, 1966)$

4.4.5 Configuration 5

Keeping configuration 4, but with end-to-end message privacy protection switched off (encryption is removed), we get the following security profile (Figure 4.4.5):

Transfering between lcl1 and ca: Average transfer-rate: $\frac{25866130}{11,2} = 2309,48KB/sec$
Transfering between lcl1 and lcl4: Average transfer-rate: $\frac{25866130}{6,3} = 4105,73KB/sec$
Average transfer-rate: $\frac{2309,48+4105,73}{2} = 3207,61KB/sec$

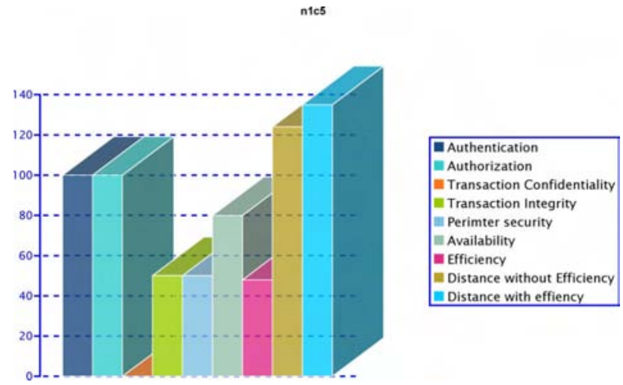

Figure 7: Network 1, measurement 5

Vectors:
$n1c5 = (100, 100, 0, 50, 50, 80)$
$n1c5e = (100, 100, 0, 50, 50, 80, 3207)$

4.4.6 Configuration 6

Keeping configuration 5, but with end-to-end message integrity protection removed, we get the following security profile (Figure 4.4.6):

Transfering between lcl1 and ca: Average transfer-rate: $\frac{25866130}{5,3} = 4880,40KB/sec$
Transfering between lcl1 and lcl4: Average transfer-rate: $\frac{25866130}{4,3} = 6015,38KB/sec$
Average transfer-rate: $\frac{4880,40+6015,38}{2} = 5447,89KB/sec$

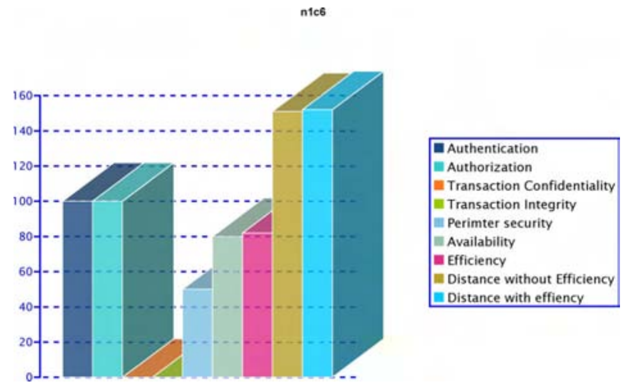

Figure 8: Network 1, measurement 1

Vectors:
$n1c6 = (100, 100, 0, 0, 50, 80)$
$n1c6e = (100, 100, 0, 0, 50, 80, 5447)$

4.5 Network 2

4.5.1 Configuration 1

We revert to network 1 with configuration 1. The direct connection between lcl1 and lcl4 is removed, and so is the direct connection between lcl2 and lcl3. The network topology is shown in Figure 9, and the security profile is shown in Figure 4.5.1.

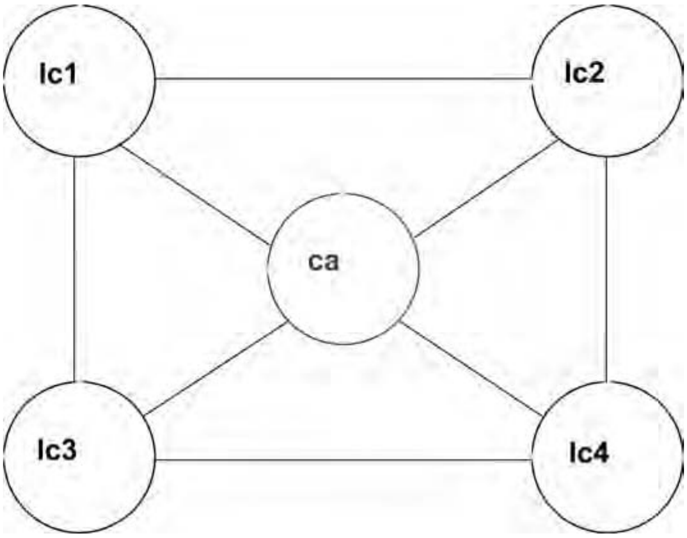

Figure 9: Network 2

Transfering between lcl1 and lcl4 with ca as intermediate node: Average transfer-rate: $\frac{25866130}{24,8} = 1042,98 KB/sec$
Transfering between lcl1 and lcl4 with lcl2 as intermediate node: Average transfer-rate: $\frac{25866130}{16,1} = 1606,59 KB/sec$
Transfering between lcl1 and lcl4 with lcl3 as intermediate node: Average transfer-rate: $\frac{25866130}{17,2} = 1503,84 KB/sec$
Average transfer-rate: $\frac{1042,98+1606,59+1503,84}{3} = 1384,47 KB/sec$

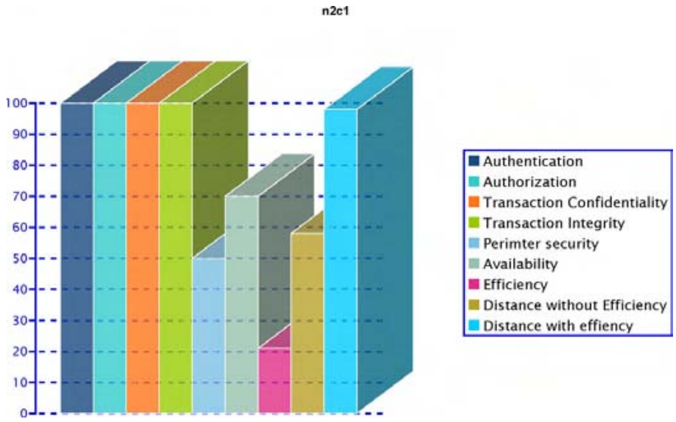

Figure 10: Network 2, measurement 1

Vectors:
$n2c1 = (100, 100, 100, 100, 50, 70)$
$n2c1e = (100, 100, 100, 100, 50, 70, 1384)$

4.5.2 Configuration 2

We keep network 2, configuration 1, but simulating policy changes in lcl2. Lcl2 no longer accepts encrypted material to enter or pass trough the node. The result is the absence of end-to-end confidentiality when messages are sent to lcl2 or pass trough lcl2 on their way (Lcl2 no longer supports/requires end-to-end confidentiality).

Transfering between lcl1 and lcl4 with ca as intermediate node: Average transfer-rate:
$\frac{25866130}{24,8} = 1042,98KB/sec$
Transfering between lcl1 and lcl4 with lcl2 as intermediate node: Average transfer-rate:
$\frac{25866130}{15,4} = 1679,62KB/sec$
Transfering between lcl1 and lcl4 with lcl3 as intermediate node: Average transfer-rate:
$\frac{25866130}{17,2} = 1503,84KB/sec$
Average transfer-rate: $\frac{1042,98+1679,62+1503,84}{3} = 1408,81KB/sec$

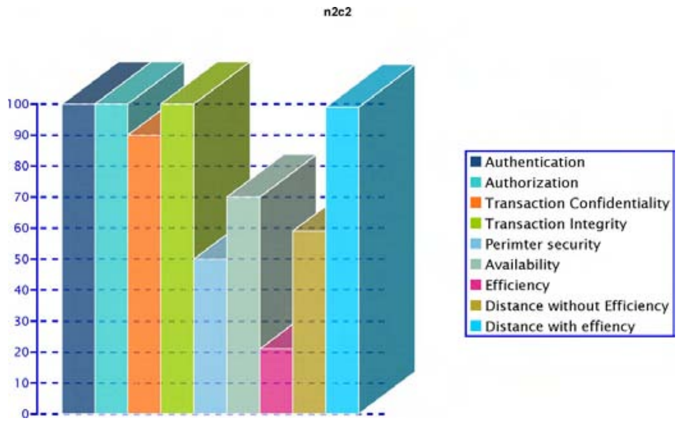

Figure 11: Network 2, measurement 2

Vectors:
$n2c2 = (100, 100, 90, 100, 50, 70)$
$n2c2e = (100, 100, 90, 100, 50, 70, 1408)$

4.5.3 Configuration 3

We keep network 2, configuration 2, but simulating policy changes in ca. Ca no longer accepts encrypted material to enter or pass trough the node. The result is the absence end-to-end confidentiality when messages are sent to ca, or pass trough ca on their way. (ca no longer supports/requires end-to-end confidentiality)

Transfering between lcl1 and lcl4 with ca as intermediate node: Average transfer-rate:
$\frac{25866130}{24,8} = 1042,98KB/sec$
Transfering between lcl1 and lcl4 with lcl2 as intermediate node: Average transfer-rate:
$\frac{25866130}{15,4} = 1679,62KB/sec$
Transfering between lcl1 and lcl4 with lcl3 as intermediate node: Average transfer-rate:
$\frac{25866130}{17,2} = 1503,84KB/sec$
Average transfer-rate: $\frac{1042,98+1679,62+1503,84}{3} = 1408,81KB/sec$
Vectors:
$n2c3 = (100, 100, 90, 100, 50, 70)$
$n2c3e = (100, 100, 90, 100, 50, 70, 1474)$

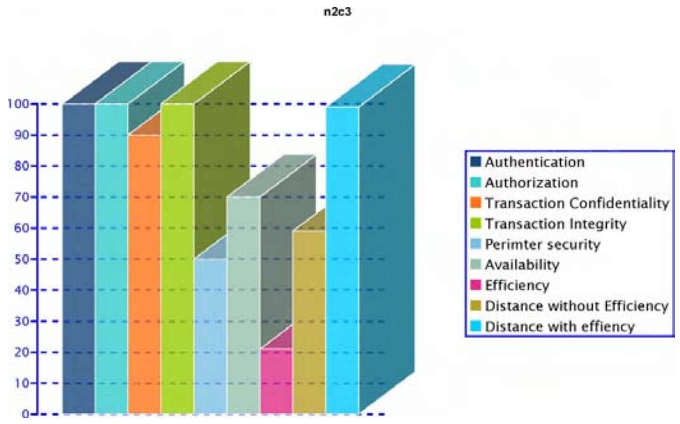

Figure 12: Network 2, measurement 3

4.5.4 Configuration 4

We keep network 2, configuration 3, but end-to-end confidentiality support is removed from all the nodes.

Transfering between lcl1 and lcl4 with ca as intermediate node: Average transfer-rate: $\frac{25866130}{24,8} = 1042,98 KB/sec$
Transfering between lcl1 and lcl4 with lcl2 as intermediate node: Average transfer-rate: $\frac{25866130}{15,4} = 1679,62 KB/sec$
Transfering between lcl1 and lcl4 with lcl3 as intermediate node: Average transfer-rate: $\frac{25866130}{15,2} = 1701,71 KB/sec$
Average transfer-rate: $\frac{1042,98+1679,62+1701,71}{3} = 1474,77 KB/sec$

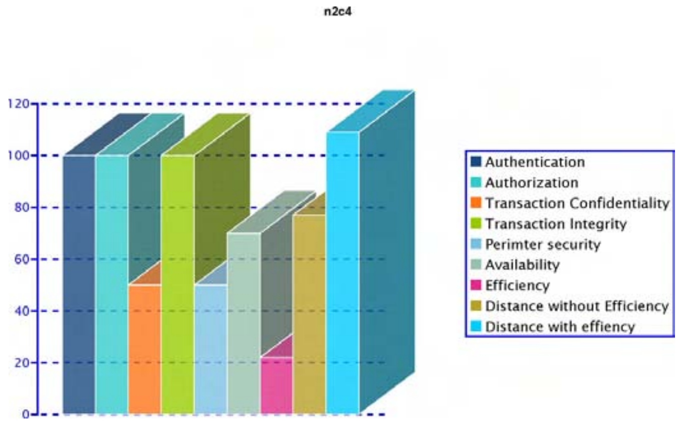

Figure 13: Network 2, measurement 4

Vectors:
$n2c4 = (100, 100, 50, 100, 50, 70)$
$n2c4e = (100, 100, 50, 100, 50, 70, 1474)$

4.5.5 Configuration 5

We keep network 2, configuration 4. Support for receiving, sending and forwarding messages with integrity protection is removed from the node lcl2.

Transfering between lcl1 and lcl4 with ca as intermediate node: Average transfer-rate: $\frac{25866130}{24,8} = 1042,98 KB/sec$
Transfering between lcl1 and lcl4 with lcl2 as intermediate node: Average transfer-rate: $\frac{25866130}{13,7} = 1888,04 KB/sec$
Transfering between lcl1 and lcl4 with lcl3 as intermediate node: Average transfer-rate: $\frac{25866130}{15,2} = 1701,71 KB/sec$
Average transfer-rate: $\frac{1042,98+1888,04+1701,71}{3} = 4632,73 KB/sec$

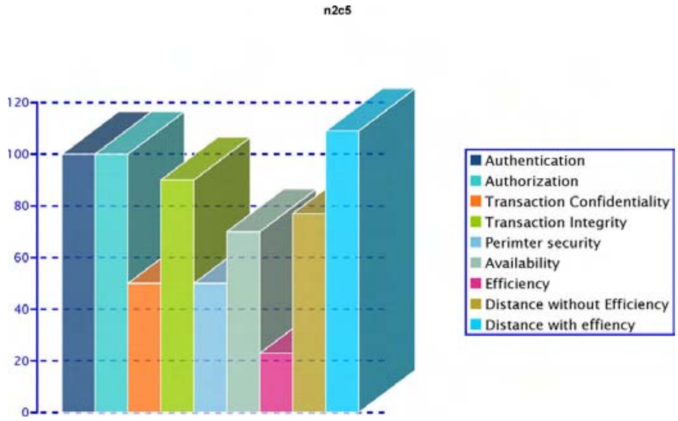

Figure 14: Network 2, measurement 5

Vectors:
$n2c5 = (100, 100, 50, 90, 50, 70)$
$n2c5e = (100, 100, 50, 90, 50, 70, 4632)$

4.5.6 Configuration 6

We keep network 2, configuration 5. Support for receiving, sending and forwarding messages with integrity protection is removed from the node lcl3.

Transfering between lcl1 and lcl4 with ca as intermediate node: Average transfer-rate: $\frac{25866130}{24,8} = 1042,98 KB/sec$
Transfering between lcl1 and lcl4 with lcl2 as intermediate node: Average transfer-rate: $\frac{25866130}{13,7} = 1888,04 KB/sec$
Transfering between lcl1 and lcl4 with lcl3 as intermediate node: Average transfer-rate: $\frac{25866130}{12,9} = 2005,13 KB/sec$
Average transfer-rate: $\frac{1042,98+1888,04+2005,13}{3} = 1645,38 KB/sec$

Vectors:
$n2c6 = (100, 100, 50, 80, 50, 70)$
$n2c6e = (100, 100, 50, 80, 50, 70, 5447)$

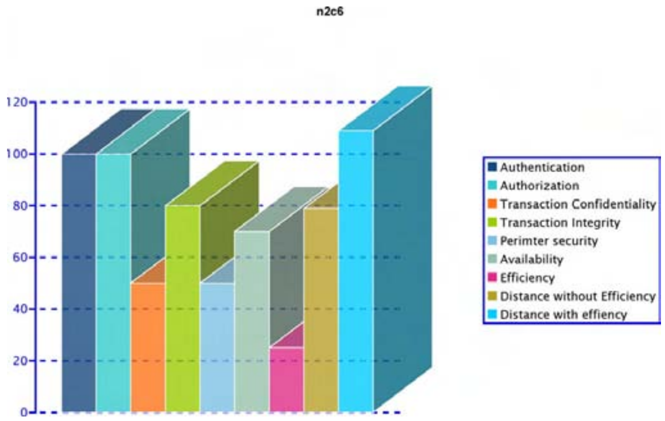

Figure 15: Network 2, measurement 6

4.5.7 Configuration 7

We keep network 2, configuration 6, but end-to-end integrity protection is removed from all the nodes.

[!ht] Transfering between lcl1 and lcl4 with ca as intermediate node:
Average transfer-rate: $\frac{25866130}{24,8} = 1042,98KB/sec$
Transfering between lcl1 and lcl4 with lcl2 as intermediate node:
Average transfer-rate: $\frac{25866130}{13,7} = 1888,04KB/sec$
Transfering between lcl1 and lcl4 with lcl3 as intermediate node:
Average transfer-rate: $\frac{25866130}{12,9} = 2005,13KB/sec$
Average transfer-rate: $\frac{1042,98+1888,04+2005,13}{3} = 1645,38KB/sec$

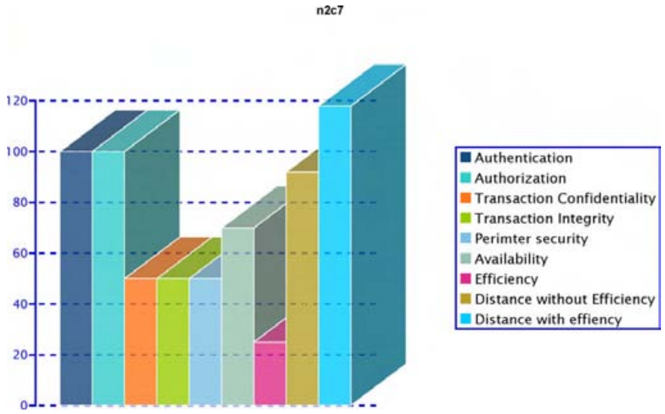

Figure 16: Network 2, measurement 7

Vectors:
$n2c7 = (100, 100, 50, 50, 50, 70)$
$n2c7e = (100, 100, 50, 50, 50, 70, 5447)$

4.5.8 Configuration 8

We revert to network 2, configuration 1. But we remove the SSH connection between lcl2 and lcl4, effectively removing communication lines security (both confidentiality and integrity) from that particular communication line.

Transfering between lcl1 and lcl4 with ca as intermediate node: Average transfer-rate: $\frac{25866130}{24,8} = 1042,98KB/sec$
Transfering between lcl1 and lcl4 with lcl2 as intermediate node: Average transfer-rate: $\frac{25866130}{8,4} = 3079,30KB/sec$
Transfering between lcl1 and lcl4 with lcl3 as intermediate node: Average transfer-rate: $\frac{25866130}{17,2} = 1503,84KB/sec$
Average transfer-rate: $\frac{1042,98+3079,30+1503,84}{3} = 1875,37KB/sec$

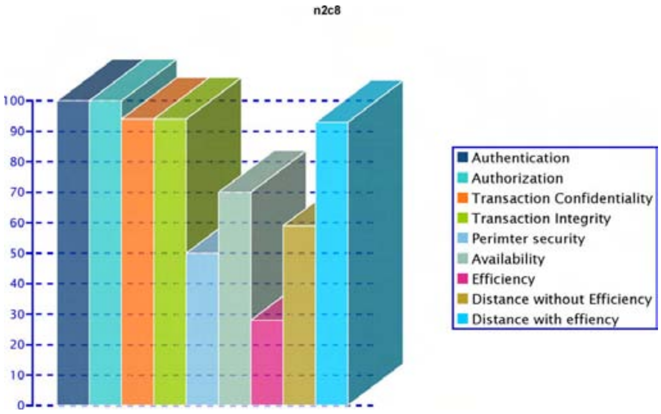

Figure 17: Network 2, measurement 8

Vectors:
$n2c8 = (100, 100, 94, 94, 50, 70)$
$n2c8e = (100, 100, 94, 94, 50, 70, 1875)$

4.5.9 Configuration 9

We keep network 2, configuration 8. But we remove the SSH connection between lcl3 and lcl4 resulting in absence of confidentiality and integrity protection on that particular communication line.

Transfering between lcl1 and lcl4 with ca as intermediate node: Average transfer-rate: $\frac{25866130}{24,8} = 1042,98KB/sec$
Transfering between lcl1 and lcl4 with lcl2 as intermediate node: Average transfer-rate: $\frac{25866130}{8,4} = 3079,30KB/sec$
Transfering between lcl1 and lcl4 with lcl3 as intermediate node: Average transfer-rate: $\frac{25866130}{8,5} = 3043,07KB/sec$
Average transfer-rate: $\frac{1042,98+3079,30+3043,07}{3} = 2388,45KB/sec$
Vectors:
$n2c9 = (100, 100, 88, 88, 50, 70)$
$n2c9e = (100, 100, 88, 88, 50, 70, 2388)$

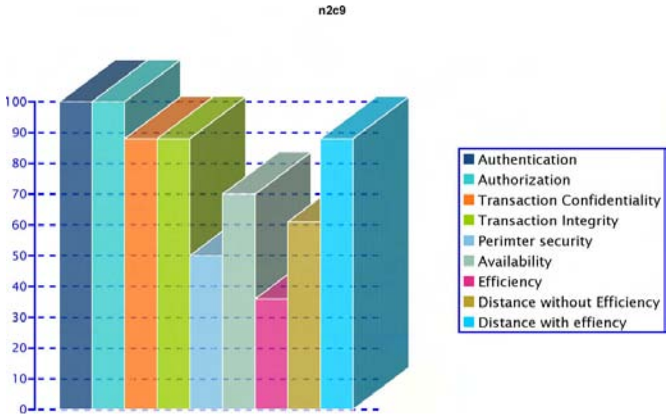

Figure 18: Network 2, measurement 9

4.5.10 Configuration 10

We keep network 2, configuration 9. But we remove the SSH connection between ca and lcl4 resulting in the absence of confidentiality and integrity protection on that particular communication line.

Transfering between lcl1 and lcl4 with ca as intermediate node: Average transfer-rate: $\frac{25866130}{8,44} = 3064,70KB/sec$
Transfering between lcl1 and lcl4 with lcl2 as intermediate node: Average transfer-rate: $\frac{25866130}{8,4} = 3079,30KB/sec$
Transfering between lcl1 and lcl4 with lcl3 as intermediate node: Average transfer-rate: $\frac{25866130}{8,5} = 3043,07KB/sec$
Average transfer-rate: $\frac{3064,70+3079,30+3043,07}{3} = 3062,35KB/sec$

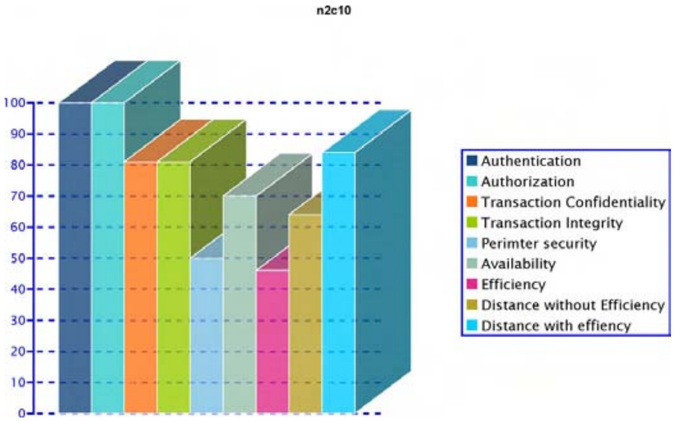

Figure 19: Network 2, measurement 10

Vectors:
$n2c10 = (100, 100, 81, 81, 50, 70)$
$n2c10e = (100, 100, 81, 81, 50, 70, 3062)$

4.5.11 Configuration 11

We keep network 2, configuration 10. Support for receiving, sending and forwarding messages with confidentiality protection is removed from the node lcl2.

Transfering between lcl1 and lcl4 with ca as intermediate node: Average transfer-rate: $\frac{25866130}{8,44} = 3064,70 KB/sec$
Transfering between lcl1 and lcl4 with lcl2 as intermediate node: Average transfer-rate: $\frac{25866130}{5,7} = 4537,92 KB/sec$
Transfering between lcl1 and lcl4 with lcl3 as intermediate node: Average transfer-rate: $\frac{25866130}{8,5} = 3043,07 KB/sec$
Average transfer-rate: $\frac{3064,70+4537,92+3043,07}{3} = 3548,56 KB/sec$

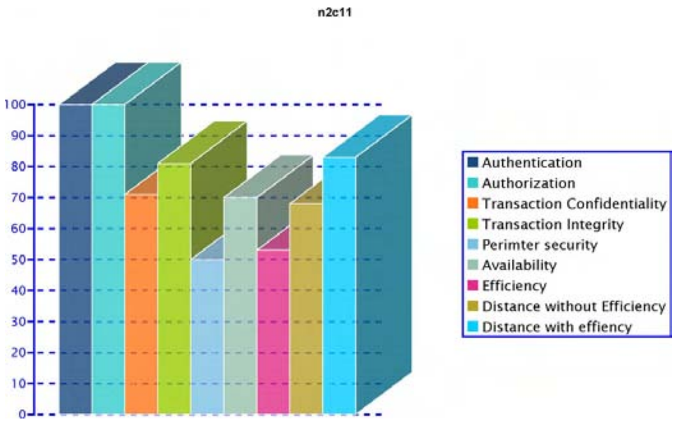

Figure 20: Network 2, measurement 11

Vectors:
$n2c11 = (100, 100, 71, 81, 50, 70)$
$n2c11e = (100, 100, 71, 81, 50, 70, 3549)$

4.5.12 Configuration 12

We keep configuration 11. Support for receiving, sending and forwarding messages with confidentiality protection is removed from the node lcl3.

Transfering between lcl1 and lcl4 with ca as intermediate node: Average transfer-rate: $\frac{25866130}{8,44} = 3064,70 KB/sec$
Transfering between lcl1 and lcl4 with lcl2 as intermediate node: Average transfer-rate: $\frac{25866130}{5,7} = 4537,92 KB/sec$
Transfering between lcl1 and lcl4 with lcl3 as intermediate node: Average transfer-rate: $\frac{25866130}{5,8} = 4459,67 KB/sec$
Average transfer-rate: $\frac{3064,70+4537,92+4459,67}{3} = 4020,76 KB/sec$
Vectors:
$n2c12 = (100, 100, 61, 81, 50, 70)$
$n2c12e = (100, 100, 61, 81, 50, 70, 4021)$

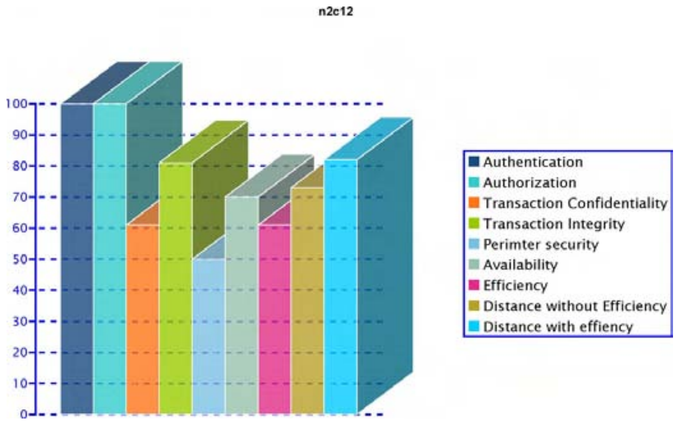

Figure 21: Network 2, measurement 12

4.5.13 Configuration 13

We keep configuration 12. Support for end-to-end confidentiality protection is removed from all the nodes.

Transfering between lcl1 and lcl4 with ca as intermediate node: Average transfer-rate: $\frac{25866130}{5,89} = 4391,53KB/sec$
Transfering between lcl1 and lcl4 with lcl2 as intermediate node: Average transfer-rate: $\frac{25866130}{5,7} = 4537,92KB/sec$
Transfering between lcl1 and lcl4 with lcl3 as intermediate node: Average transfer-rate: $\frac{25866130}{5,8} = 4459,67KB/sec$
Average transfer-rate: $\frac{4391,53+4537,92+4459,67}{3} = 4463,04KB/sec$

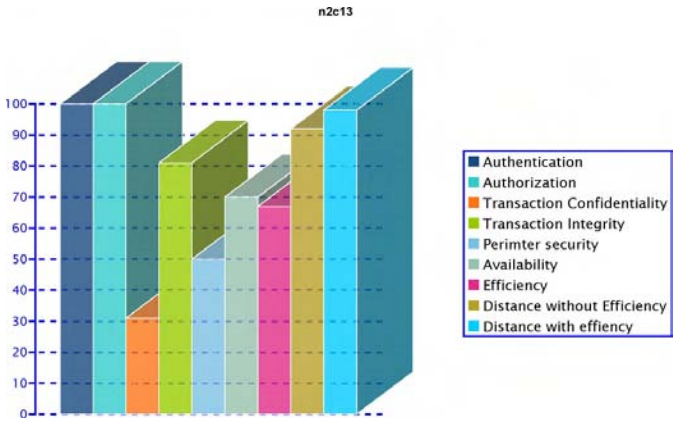

Figure 22: Network 2, measurement 13

Vectors:
$n2c13 = (100, 100, 31, 81, 50, 70)$
$n2c13e = (100, 100, 31, 81, 50, 70, 4463)$

4.5.14 Configuration 14

We keep configuration 13. Support for receiving, sending and forwarding messages with integrity protection is removed from the node lcl2.

Transfering between lcl1 and lcl4 with ca as intermediate node: Average transfer-rate: $\frac{25866130}{5,89} = 4391,53KB/sec$
Transfering between lcl1 and lcl4 with lcl2 as intermediate node: Average transfer-rate: $\frac{25866130}{4.0} = 6466,53KB/sec$
Transfering between lcl1 and lcl4 with lcl3 as intermediate node: Average transfer-rate: $\frac{25866130}{5,8} = 4459,67KB/sec$
Average transfer-rate: $\frac{4391,53+6466,53+4459,67}{3} = 5105.91KB/sec$

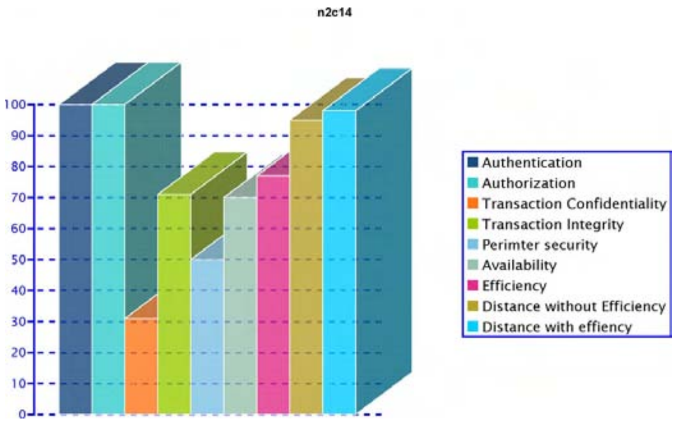

Figure 23: Network 2, measurement 14

Vectors:
$n2c14 = (100, 100, 31, 71, 50, 70)$
$n2c14e = (100, 100, 31, 71, 50, 70, 5106)$

4.5.15 Configuration 15

We keep configuration 14. Support for receiving, sending and forwarding messages with integrity protection is removed from the node lcl3.

Transfering between lcl1 and lcl4 with ca as intermediate node: Average transfer-rate: $\frac{25866130}{5,89} = 4391,53KB/sec$
Transfering between lcl1 and lcl4 with lcl2 as intermediate node: Average transfer-rate: $\frac{25866130}{4.0} = 6466,53KB/sec$
Transfering between lcl1 and lcl4 with lcl3 as intermediate node: Average transfer-rate: $\frac{25866130}{3,9} = 6632,34KB/sec$
Average transfer-rate: $\frac{4391,53+6466,53,92+6632,34}{3} = 5830.13KB/sec$
Vectors:
$n2c15 = (100, 100, 31, 61, 50, 70)$
$n2c15e = (100, 100, 31, 61, 50, 70, 5830)$

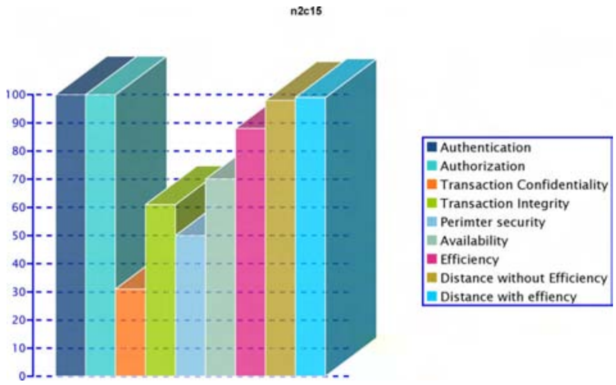

Figure 24: Network 2, measurement 15

4.5.16 Configuration 16

We keep configuration 15. Support for end-to-end integrity protection is removed from all the nodes.

Transfering between lcl1 and lcl4 with ca as intermediate node: Average transfer-rate: $\frac{25866130}{3,8} = 6806,87 KB/sec$
Transfering between lcl1 and lcl4 with lcl2 as intermediate node: Average transfer-rate: $\frac{25866130}{4.0} = 6466,53 KB/sec$
Transfering between lcl1 and lcl4 with lcl3 as intermediate node: Average transfer-rate: $\frac{25866130}{3,9} = 6632,34 KB/sec$
Average transfer-rate: $\frac{6806,87+6466,53+6632,34}{3} = 6635,24, KB/sec$

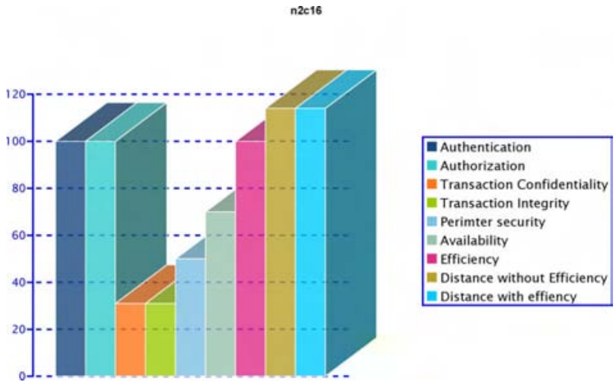

Figure 25: Network 2, measurement 16

Vectors:
$n2c16 = (100, 100, 31, 31, 50, 70)$
$n2c16e = (100, 100, 31, 31, 50, 70, 6635)$

4.6 Network 3

We revert to network 2, configuration 1. But we remove the connection between lcl1 and ca, and the connection between lcl2 and lcl4. All the communication lines are both confidentiality and integrity protected and all the nodes suppport and use end-to-end security. The topology of network 3 can be found in Figure 26.

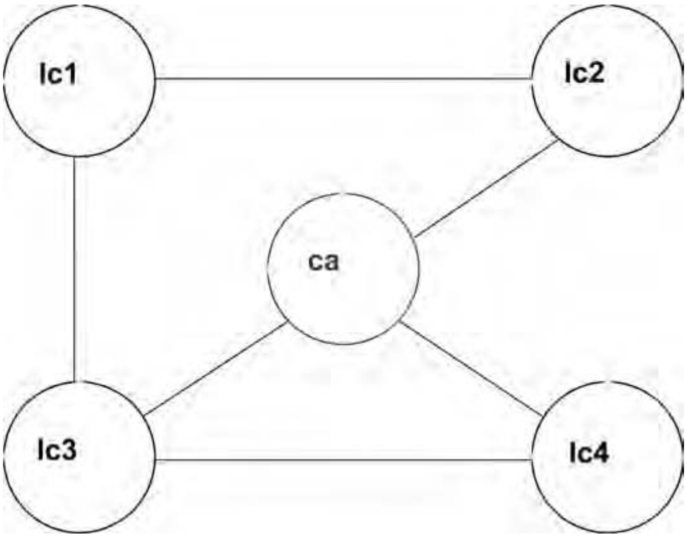

Figure 26: Network 3

4.6.1 Configuration 1

Transfering between lcl1 and lcl4 with lcl2 and ca as intermediate nodes: Average transfer-rate: $\frac{25866130}{25{,}49} = 1014{,}76KB/sec$
Transfering between lcl1 and lcl4 with lcl3 as intermediate node: Average transfer-rate: $\frac{25866130}{17{,}33} = 1492{,}56KB/sec$
Transfering between lcl1 and lcl4 with lcl3 and ca as intermediate nodes: Average transfer-rate: $\frac{25866130}{25{,}11} = 1030{,}11KB/sec$
Average transfer-rate: $\frac{1014{,}76+1492{,}56+1030{,}11}{3} = 1179{,}14KB/sec$

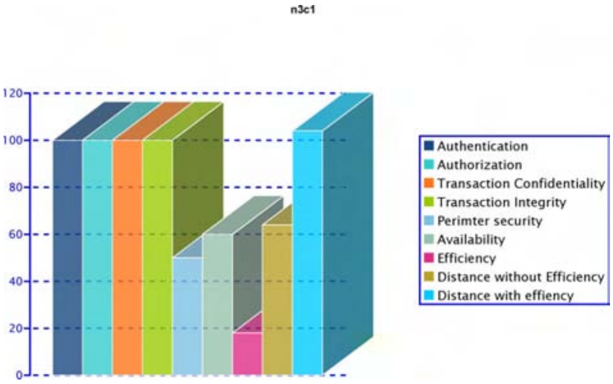

Figure 27: Network 3, measurement 1

Vectors:
$n3c1 = (100, 100, 100, 100, 50, 60)$
$n3c1e = (100, 100, 100, 100, 50, 60, 1179)$

4.6.2 Configuration 2

We keep network 3, configuration 1. Support for receiving, sending and forwarding messages with confidentiality protection is removed from the node lcl3.

Transfering between lcl1 and lcl4 with lcl2 and ca as intermediate nodes: Average transfer-rate: $\frac{25866130}{25{,}49} = 1014{,}76KB/sec$
Transfering between lcl1 and lcl4 with lcl3 as intermediate node: Average transfer-rate: $\frac{25866130}{14{,}89} = 1737{,}15KB/sec$
Transfering between lcl1 and lcl4 with lcl3 and ca as intermediate nodes: Average transfer-rate: $\frac{25866130}{25{,}00} = 1034{,}65KB/sec$
Average transfer-rate: $\frac{1014{,}76+1737{,}15+1034{,}65}{3} = 1262{,}19KB/sec$

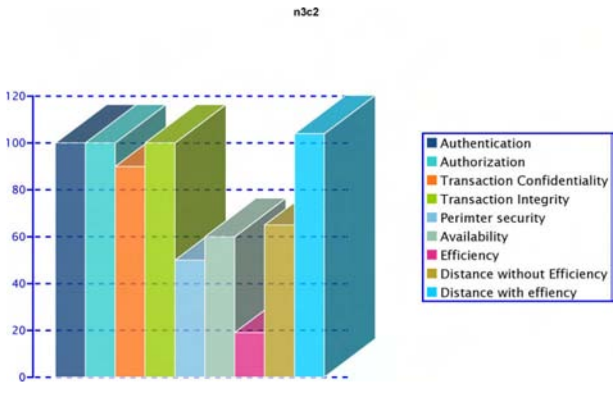

Figure 28: Network 3, measurement 2

Vectors:
$n3c2 = (100, 100, 90, 100, 50, 60)$
$n3c2e = (100, 100, 90, 100, 50, 60, 1262)$

4.6.3 Configuration 3

We keep network 3, configuration 2. Support for receiving, sending and forwarding messages with confidentiality protection is removed from the node ca.

Transfering between lcl1 and lcl4 with lcl2 and ca as intermediate nodes: Average transfer-rate: $\frac{25866130}{25{,}23} = 1025{,}21KB/sec$
Transfering between lcl1 and lcl4 with lcl3 as intermediate node: Average transfer-rate: $\frac{25866130}{14{,}89} = 1737{,}15KB/sec$
Transfering between lcl1 and lcl4 with lcl3 and ca as intermediate nodes: Average transfer-rate: $\frac{25866130}{25{,}00} = 1034{,}65KB/sec$
Average transfer-rate: $\frac{1025{,}21+1737{,}15+1034{,}65}{3} = 1265{,}67KB/sec$
Vectors:
$n3c3 = (100, 100, 80, 100, 50, 60)$
$n3c3e = (100, 100, 80, 100, 50, 60, 1266)$

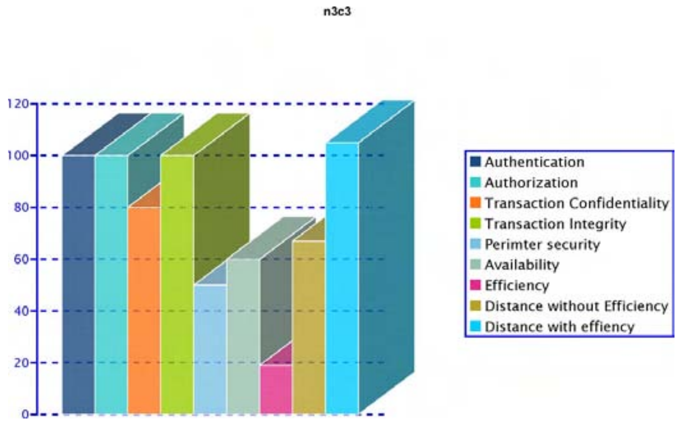

Figure 29: Network 3, measurement 3

4.6.4 Configuration 4

We keep network 3, configuration 3. Support for receiving, sending and forwarding messages with confidentiality protection is removed from the node lcl2.

Transfering between lcl1 and lcl4 with lcl2 and ca as intermediate nodes: Average transfer-rate: $\frac{25866130}{25,23} = 1025,21KB/sec$
Transfering between lcl1 and lcl4 with lcl3 as intermediate node: Average transfer-rate: $\frac{25866130}{14,89} = 1737,15KB/sec$
Transfering between lcl1 and lcl4 with lcl3 and ca as intermediate nodes: Average transfer-rate: $\frac{25866130}{25,00} = 1034,65KB/sec$
Average transfer-rate: $\frac{1025,21+1737,15+1034,65}{3} = 1265,67KB/sec$

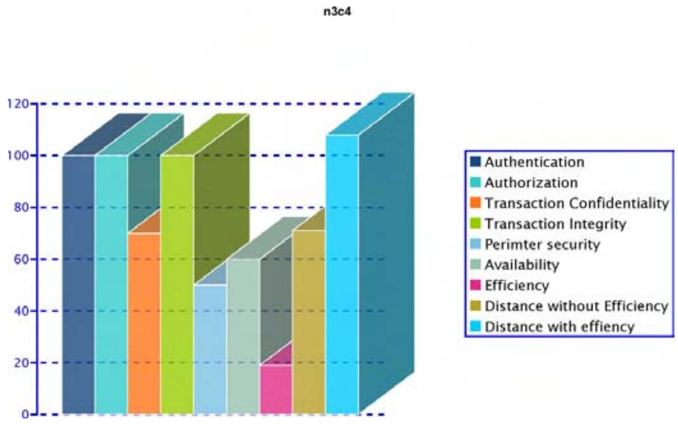

Figure 30: Network 3, measurement 4

Vectors:
$n3c4 = (100, 100, 70, 100, 50, 60)$
$n3c4e = (100, 100, 70, 100, 50, 60, 1266)$

4.6.5 Configuration 5

We keep network 3, configuration 4. Support for receiving, sending and forwarding messages with integrity protection is removed from the node lcl3.

Transfering between lcl1 and lcl4 with lcl2 and ca as intermediate nodes: Average transfer-rate: $\frac{25866130}{25{,}23} = 1025{,}21KB/sec$
Transfering between lcl1 and lcl4 with lcl3 as intermediate node: Average transfer-rate: $\frac{25866130}{13{,}00} = 1989{,}70KB/sec$
Transfering between lcl1 and lcl4 with lcl3 and ca as intermediate nodes: Average transfer-rate: $\frac{25866130}{25{,}03} = 1033{,}40KB/sec$
Average transfer-rate: $\frac{1025{,}21+1989{,}70+1033{,}40}{3} = 1349{,}44KB/sec$

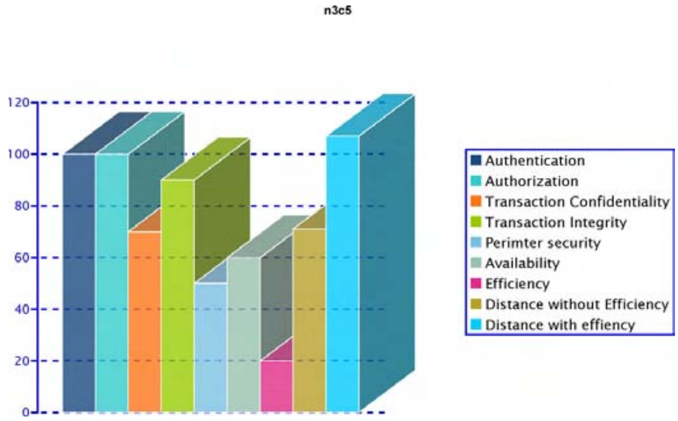

Figure 31: Network 3, measurement 5

Vectors:
$n3c5 = (100, 100, 70, 90, 50, 60)$
$n3c5e = (100, 100, 70, 90, 50, 60, 1349)$

4.6.6 Configuration 6

We keep network 3, configuration 5. Support for receiving, sending and forwarding messages with integrity protection is removed from the node ca.

Transfering between lcl1 and lcl4 with lcl2 and ca as intermediate nodes: Average transfer-rate: $\frac{25866130}{25{,}85} = 1000{,}62KB/sec$
Transfering between lcl1 and lcl4 with lcl3 as intermediate node: Average transfer-rate: $\frac{25866130}{13{,}00} = 1989{,}70KB/sec$
Transfering between lcl1 and lcl4 with lcl3 and ca as intermediate nodes: Average transfer-rate: $\frac{25866130}{25{,}03} = 1033{,}40KB/sec$
Average transfer-rate: $\frac{1000{,}62+1989{,}70+1033{,}40}{3} = 1341{,}24KB/sec$
Vectors:
$n3c6 = (100, 100, 70, 80, 50, 60)$
$n3c6e = (100, 100, 70, 80, 50, 60, 1341)$

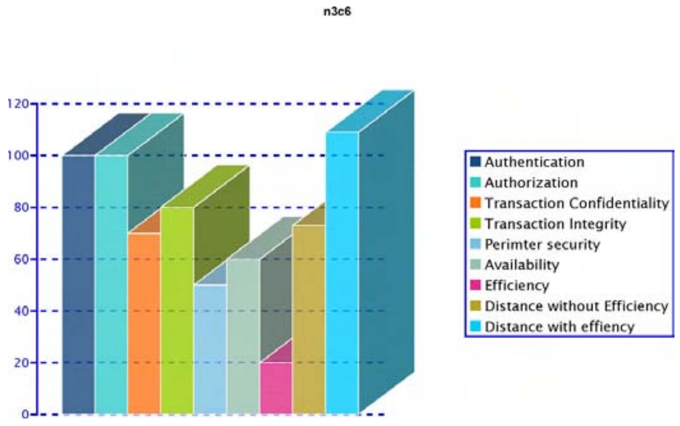

Figure 32: Network 3, measurement 6

4.6.7 Configuration 7

We keep network 3, configuration 6. Support for receiving, sending and forwarding messages with integrity protection is removed from the node lcl2.

Transfering between lcl1 and lcl4 with lcl2 and ca as intermediate nodes: Average transfer-rate: $\frac{25866130}{25,85} = 1000,62KB/sec$
Transfering between lcl1 and lcl4 with lcl3 as intermediate node: Average transfer-rate: $\frac{25866130}{13,00} = 1989,70KB/sec$
Transfering between lcl1 and lcl4 with lcl3 and ca as intermediate nodes: Average transfer-rate: $\frac{25866130}{25,03} = 1033,40KB/sec$
Average transfer-rate: $\frac{1000,62+1989,70+1033,40}{3} = 1341,24KB/sec$

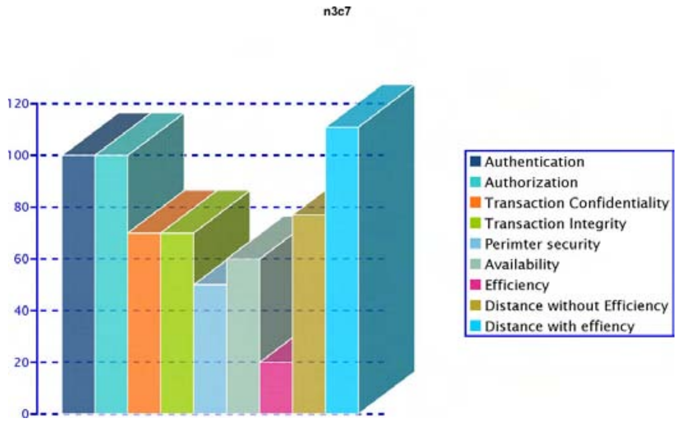

Figure 33: Network 3, measurement 7

Vectors:
$n3c7 = (100, 100, 70, 70, 50, 60)$
$n3c7e = (100, 100, 70, 70, 50, 60, 1341)$

4.6.8 Configuration 8

We revert to network 3, configuration 1. The SSH connection between ca and lcl4 is removed.

Transfering between lcl1 and lcl4 with lcl2 and ca as intermediate nodes: Average transfer-rate: $\frac{25866130}{10,03} = 2578,87KB/sec$
Transfering between lcl1 and lcl4 with lcl3 as intermediate node: Average transfer-rate: $\frac{25866130}{17,33} = 1492,57KB/sec$
Transfering between lcl1 and lcl4 with lcl3 and ca as intermediate nodes: Average transfer-rate: $\frac{25866130}{8,82} = 2932,67KB/sec$
Average transfer-rate: $\frac{2578,87+1492,57+2932,67}{3} = 2334,70KB/sec$

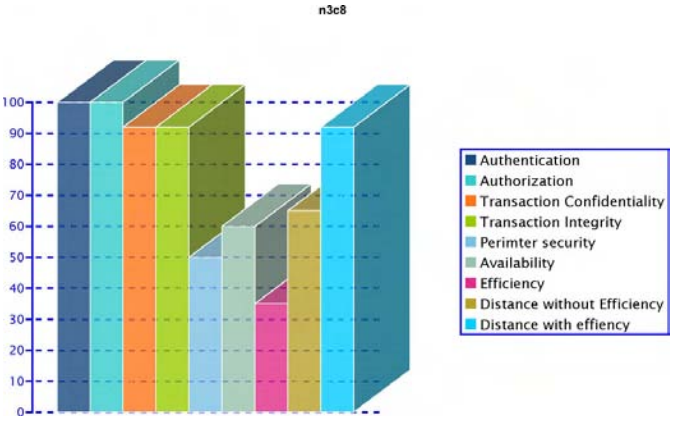

Figure 34: Network 3, measurement 8

Vectors:
$n3c8 = (100, 100, 92, 92, 50, 60)$
$n3c8e = (100, 100, 92, 92, 50, 60, 2335)$

4.6.9 Configuration 9

We keep network 3, configuration 8. The SSH connection between lcl3 and lcl4 is removed.

Transfering between lcl1 and lcl4 with lcl2 and ca as intermediate nodes: Average transfer-rate: $\frac{25866130}{10,03} = 2578,87KB/sec$
Transfering between lcl1 and lcl4 with lcl3 as intermediate node: Average transfer-rate: $\frac{25866130}{8,98} = 2880,42KB/sec$
Transfering between lcl1 and lcl4 with lcl3 and ca as intermediate nodes: Average transfer-rate: $\frac{25866130}{8,82} = 2932,67KB/sec$
Average transfer-rate: $\frac{2578,87+2880,42+2932,67}{3} = 2800,32KB/sec$
Vectors:
$n3c9 = (100, 100, 83, 83, 50, 60)$
$n3c9e = (100, 100, 83, 83, 50, 60, 2800)$

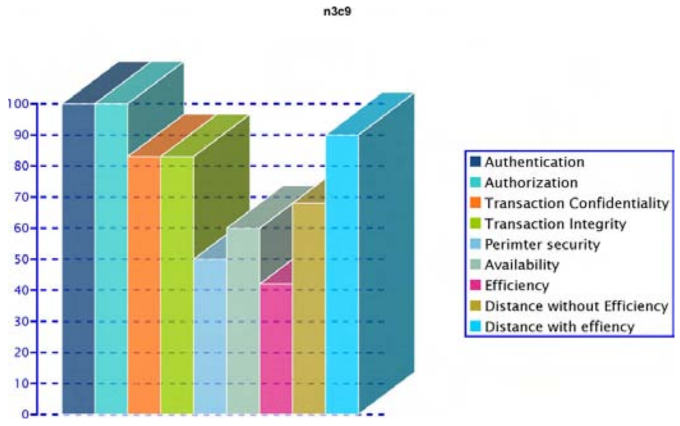

Figure 35: Network 3, measurement 9

4.6.10 Configuration 10

We keep network 3, configuration 9. Support for receiving, sending and forwarding messages with confidentiality protection is removed from the node lcl3.

Transfering between lcl1 and lcl4 with lcl2 and ca as intermediate nodes: Average transfer-rate: $\frac{25866130}{10,03} = 2578,87KB/sec$
Transfering between lcl1 and lcl4 with lcl3 as intermediate node: Average transfer-rate: $\frac{25866130}{5,72} = 4522,05KB/sec$
Transfering between lcl1 and lcl4 with lcl3 and ca as intermediate nodes: Average transfer-rate: $\frac{25866130}{6,07} = 4261,31KB/sec$
Average transfer-rate: $\frac{2578,87+4522,05+4261,31}{3} = 3787,41KB/sec$

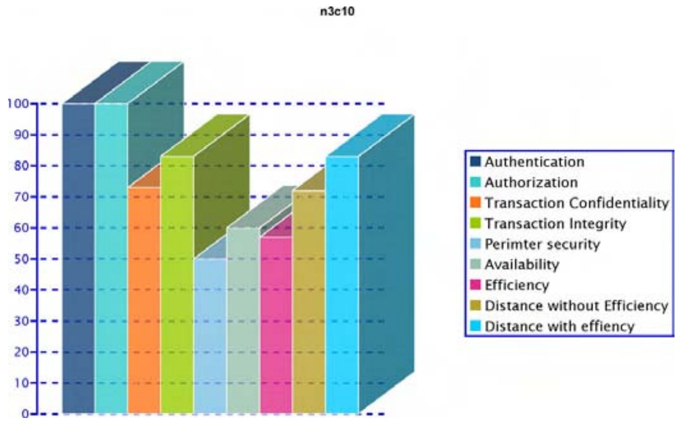

Figure 36: Network 3, measurement 10

Vectors:
$n3c10 = (100, 100, 73, 83, 50, 60)$
$n3c10e = (100, 100, 73, 83, 50, 60, 3787)$

4.6.11 Configuration 11

We keep network 3, configuration 10. Support for receiving, sending and forwarding messages with confidentiality protection is removed from the node ca.

Transfering between lcl1 and lcl4 with lcl2 and ca as intermediate nodes: Average transfer-rate: $\frac{25866130}{6,49} = 3985,54KB/sec$
Transfering between lcl1 and lcl4 with lcl3 as intermediate node: Average transfer-rate: $\frac{25866130}{5,72} = 4522,05KB/sec$
Transfering between lcl1 and lcl4 with lcl3 and ca as intermediate nodes: Average transfer-rate: $\frac{25866130}{6,07} = 4261,31KB/sec$
Average transfer-rate: $\frac{3985,54+4522,05+4261,31}{3} = 4256,30KB/sec$

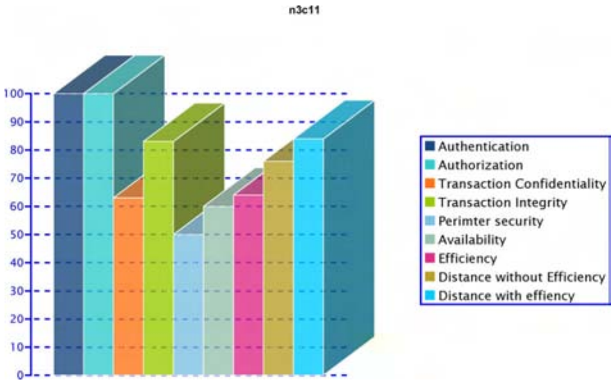

Figure 37: Network 3, measurement 11

Vectors:
$n3c11 = (100, 100, 63, 83, 50, 60)$
$n3c11e = (100, 100, 63, 83, 50, 60, 4256)$

4.6.12 Configuration 12

We keep network 3, configuration 11. Support for receiving, sending and forwarding messages with confidentiality protection is removed from the node lcl2.

Transfering between lcl1 and lcl4 with lcl2 and ca as intermediate nodes: Average transfer-rate: $\frac{25866130}{6,49} = 3985,54KB/sec$
Transfering between lcl1 and lcl4 with lcl3 as intermediate node: Average transfer-rate: $\frac{25866130}{5,72} = 4522,05KB/sec$
Transfering between lcl1 and lcl4 with lcl3 and ca as intermediate nodes: Average transfer-rate: $\frac{25866130}{6,07} = 4261,31KB/sec$
Average transfer-rate: $\frac{3985,54+4522,05+4261,31}{3} = 4256,30KB/sec$
Vectors:
$n3c12 = (100, 100, 53, 83, 50, 60)$
$n3c12e = (100, 100, 53, 83, 50, 60, 4256)$

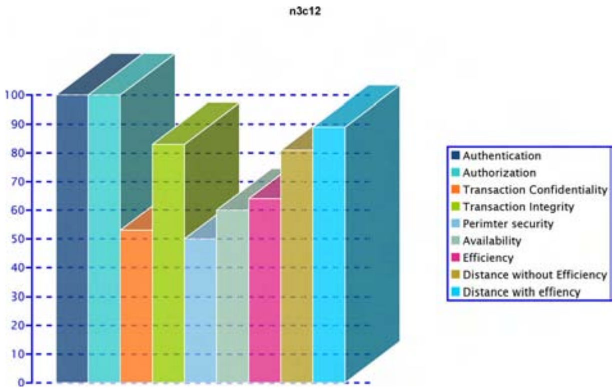

Figure 38: Network 3, measurement 12

4.6.13 Configuration 13

We keep network 3, configuration 12. Support for receiving, sending and forwarding messages with integrity protection is removed from the the node lcl3.

Transfering between lcl1 and lcl4 with lcl2 and ca as intermediate nodes: Average transfer-rate: $\frac{25866130}{6,49} = 3985,54KB/sec$
Transfering between lcl1 and lcl4 with lcl3 as intermediate node: Average transfer-rate: $\frac{25866130}{3,81} = 6789,01KB/sec$
Transfering between lcl1 and lcl4 with lcl3 and ca as intermediate nodes: Average transfer-rate: $\frac{25866130}{3,97} = 6515,40KB/sec$
Average transfer-rate: $\frac{3985,54+6789,01+6515,40}{3} = 5763,31KB/sec$

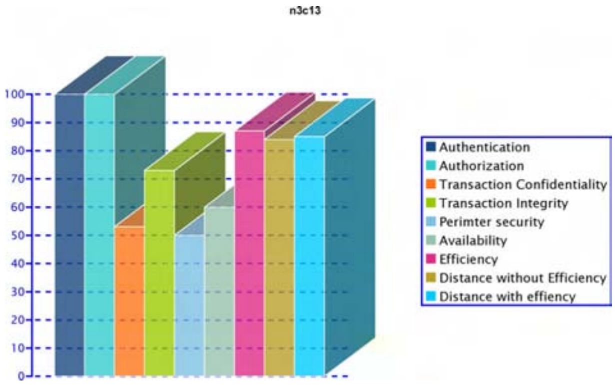

Figure 39: Network 3, measurement 13

Vectors:
$n3c13 = (100, 100, 53, 73, 50, 60)$
$n3c13e = (100, 100, 53, 73, 50, 60, 5763)$

4.6.14 Configuration 14

We keep network 3, configuration 13. Support for receiving, sending and forwarding messages with integrity protection is removed from the node ca.

Transfering between lcl1 and lcl4 with lcl2 and ca as intermediate nodes: Average transfer-rate: $\frac{25866130}{4,21} = 6143,97 KB/sec$
Transfering between lcl1 and lcl4 with lcl3 as intermediate node: Average transfer-rate: $\frac{25866130}{3,81} = 6789,01 KB/sec$
Transfering between lcl1 and lcl4 with lcl3 and ca as intermediate nodes: Average transfer-rate: $\frac{25866130}{3,97} = 6515,40 KB/sec$
Average transfer-rate: $\frac{6143,97+6789,01+6515,40}{3} = 6482,79 KB/sec$

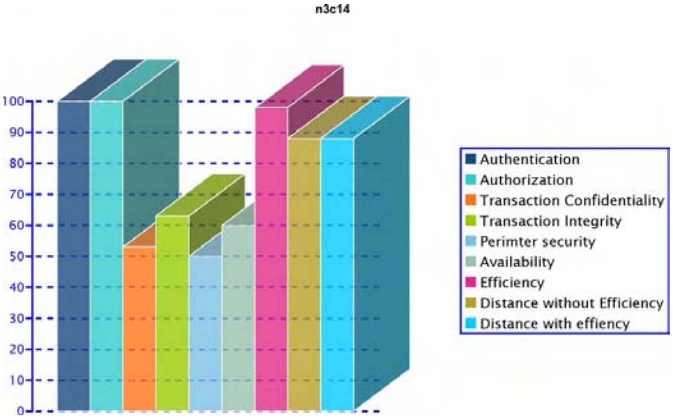

Figure 40: Network 3, measurement 14

Vectors:
$n3c14 = (100, 100, 53, 63, 50, 60)$
$n3c14e = (100, 100, 53, 63, 50, 60, 6482)$

4.6.15 Configuration 15

We keep network 3, configuration 14. Support for receiving, sending and forwarding messages with integrity protection is removed from the node lcl2.

Transfering between lcl1 and lcl4 with lcl2 and ca as intermediate nodes: Average transfer-rate: $\frac{25866130}{4,21} = 6143,97 KB/sec$
Transfering between lcl1 and lcl4 with lcl3 as intermediate node: Average transfer-rate: $\frac{25866130}{3,81} = 6789,01 KB/sec$
Transfering between lcl1 and lcl4 with lcl3 and ca as intermediate nodes: Average transfer-rate: $\frac{25866130}{3,97} = 6515,40 KB/sec$
Average transfer-rate: $\frac{6143,97+6789,01+6515,40}{3} = 6482,79 KB/sec$
Vectors:
$n3c15 = (100, 100, 53, 53, 50, 60)$
$n3c15e = (100, 100, 53, 53, 50, 60, 6483)$

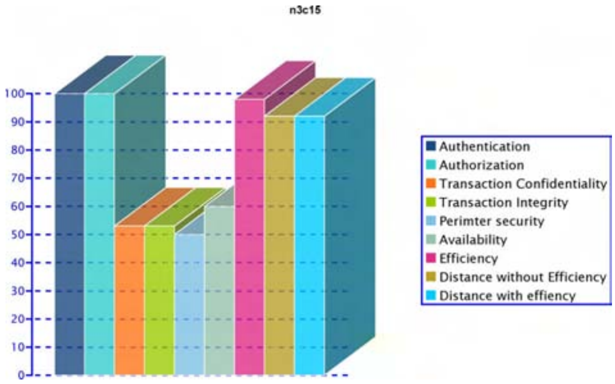

Figure 41: Network 3, measurement 15

4.7 Network 4

We revert to network 3, configuration 1. We remove the direct connection between lcl3 and lcl4. The network topography is given in Figure 42

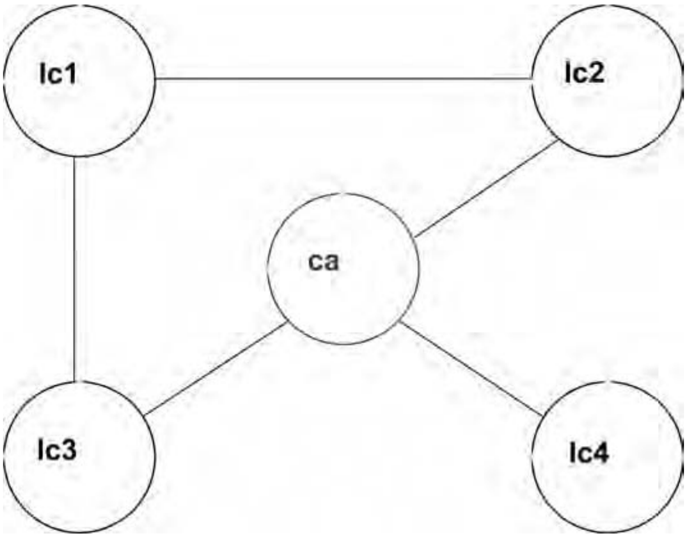

Figure 42: Network 4

4.7.1 Configuration 1

Transfering between lcl1 and lcl4 with lcl2 and ca as intermediate nodes: Average transfer-rate: $\frac{25866130}{25,49} = 1014,76KB/sec$
Transfering between lcl1 and lcl4 with lcl3 and ca as intermediate node: Average transfer-rate: $\frac{25866130}{25,11} = 1030,11KB/sec$
Average transfer-rate: $\frac{1014,76+1030,11}{2} = 1022,44KB/sec$
Vectors:
$n4c1 = (100, 100, 100, 100, 50, 55)$
$n4c1e = (100, 100, 100, 100, 50, 55, 1022)$

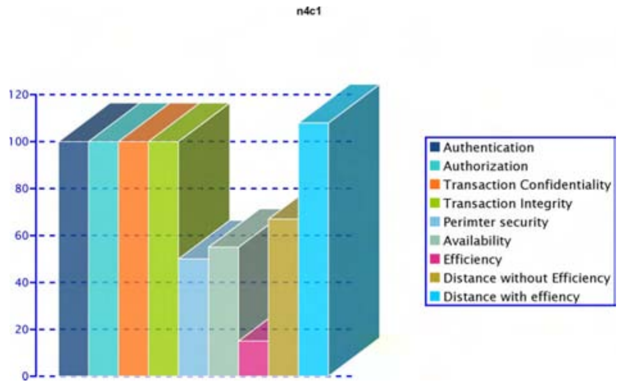

Figure 43: Network 4, measurement 1

4.7.2 Configuration 2

We keep configuration 1. Support for receiving, sending and forwarding messages with confidentiality protection is removed from the node lc3.

Transfering between lcl1 and lcl4 with lcl2 and ca as intermediate nodes: Average transfer-rate: $\frac{25866130}{25,23} = 1025,21 KB/sec$
Transfering between lcl1 and lcl4 with lcl3 and ca as intermediate node: Average transfer-rate: $\frac{25866130}{25,11} = 1030,11 KB/sec$
Average transfer-rate: $\frac{1025,21+1035,06}{2} = 1027,66 KB/sec$

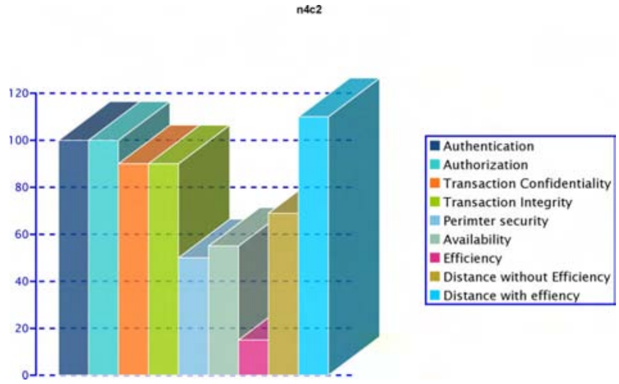

Figure 44: Network 4, measurement 2

Vectors:
$n4c2 = (100, 100, 80, 100, 50, 55)$
$n4c2e = (100, 100, 80, 100, 50, 55, 1028)$

Transfering between lcl1 and lcl4 with lcl2 and ca as intermediate nodes: Average transfer-rate: $\frac{25866130}{25,23} = 1025,21 KB/sec$
Transfering between lcl1 and lcl4 with lcl3 and ca as intermediate node: Average transfer-rate: $\frac{25866130}{24,99} = 1035,06 KB/sec$
Average transfer-rate: $\frac{1025,21+1035,06}{2} = 1030,14 KB/sec$

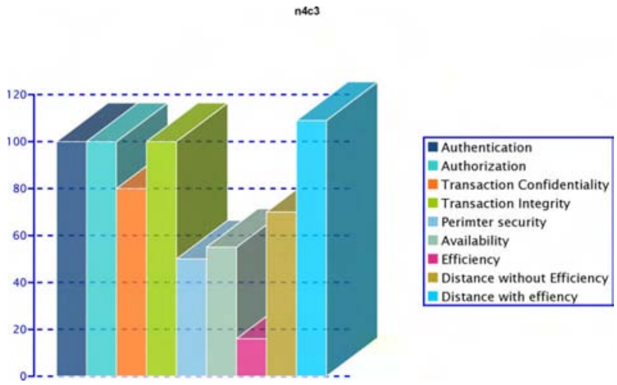

Figure 45: Network 4, measurement 3

Vectors:
$n4c3 = (100, 100, 80, 100, 50, 55)$
$n4c3e = (100, 100, 80, 100, 50, 55, 1030)$

4.7.3 Configuration 4

We keep configuration 3. Support for receiving, sending and forwarding messages with integrity protection is removed from the node lc2.

Transfering between lcl1 and lcl4 with lcl2 and ca as intermediate nodes: Average transfer-rate: $\frac{25866130}{25,85} = 1000,62KB/sec$
Transfering between lcl1 and lcl4 with lcl3 and ca as intermediate node: Average transfer-rate: $\frac{25866130}{24,99} = 1035,06KB/sec$
Average transfer-rate: $\frac{1000,62+1035,06}{2} = 1017,84KB/sec$

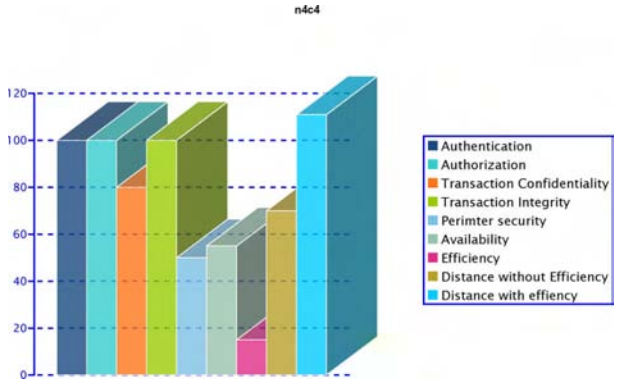

Figure 46: Network 4, measurement 4

Vectors:
$n4c4 = (100, 100, 80, 90, 50, 55)$
$n4c4e = (100, 100, 80, 90, 50, 55, 1018)$

4.7.4 Configuration 5

We keep configuration 4. Support for receiving, sending and forwarding messages with integrity protection is removed from the node lc3.

Transfering between lcl1 and lcl4 with lcl2 and ca as intermediate nodes: Average transfer-rate: $\frac{25866130}{25,85} = 1000,62\text{KB}/sec$
Transfering between lcl1 and lcl4 with lcl3 and ca as intermediate node: Average transfer-rate: $\frac{25866130}{25,03} = 1033,41\text{KB}/sec$
Average transfer-rate: $\frac{1000,62+1033,41}{2} = 1017,02\text{KB}/sec$

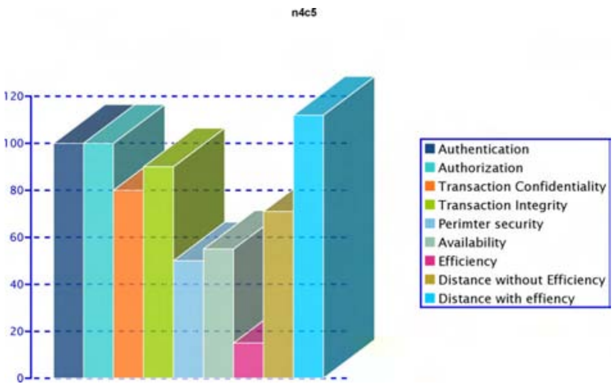

Figure 47: Network 4, measurement 5

Vectors:
$n4c5 = (100, 100, 80, 80, 50, 55)$
$n4c5e = (100, 100, 80, 80, 50, 55, 1017)$

4.7.5 Configuration 6

We revert to network 4, configuration 1. But we remove the ssh connection between ca and lcl4.

Transfering between lcl1 and lcl4 with lcl2 and ca as intermediate nodes: Average transfer-rate: $\frac{25866130}{10,03} = 2578,88\text{KB}/sec$
Transfering between lcl1 and lcl4 with lcl3 and ca as intermediate node: Average transfer-rate: $\frac{25866130}{8,82} = 2932,68\text{KB}/sec$
Average transfer-rate: $\frac{2578,88+2932,68}{2} = 2755,78\text{KB}/sec$

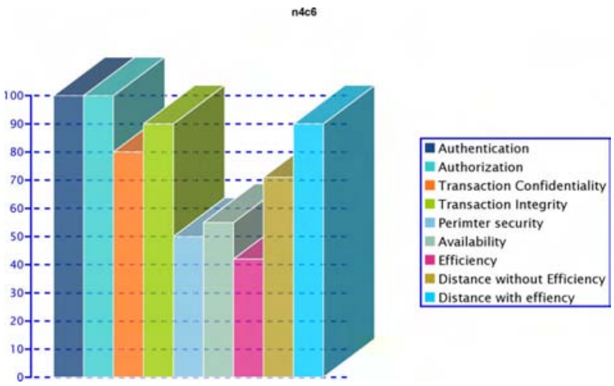

Figure 48: Network 4, measurement 6

Vectors:
$n4c6 = (100, 100, 90, 90, 50, 55)$
$n4c6e = (100, 100, 90, 90, 50, 55, 2756)$

4.7.6 Configuration 7

We keep configuration 6. Support for receiving, sending and forwarding messages with confidentiality protection is removed from the node lc2.

Transfering between lcl1 and lcl4 with lcl2 and ca as intermediate nodes: Average transfer-rate: $\frac{25866130}{6,46} = 4004,04KB/sec$
Transfering between lcl1 and lcl4 with lcl3 and ca as intermediate node: Average transfer-rate: $\frac{25866130}{8,82} = 2932,68KB/sec$
Average transfer-rate: $\frac{4004,04+2932,68}{2} = 3468,38KB/sec$

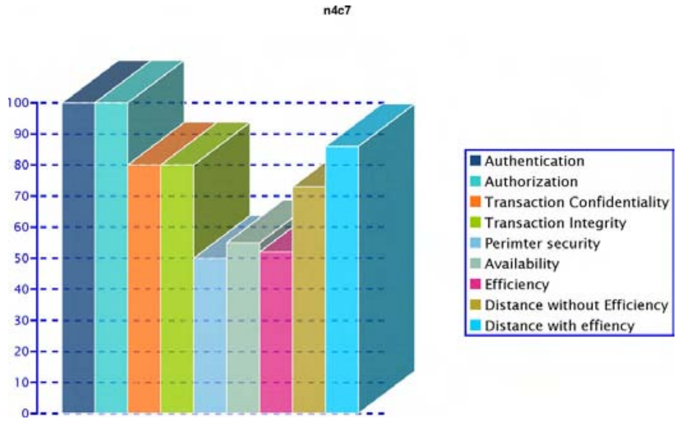

Figure 49: Network 4, measurement 7

Vectors:
$n4c7 = (100, 100, 80, 90, 50, 55)$
$n4c7e = (100, 100, 80, 90, 50, 55, 4133)$

4.7.7 Configuration 8

We keep configuration 7. Support for receiving, sending and forwarding messages with confidentiality protection is removed from the node lc3.

Transfering between lcl1 and lcl4 with lcl2 and ca as intermediate nodes: Average transfer-rate: $\frac{25866130}{6,46} = 4004,04KB/sec$
Transfering between lcl1 and lcl4 with lcl3 and ca as intermediate node: Average transfer-rate: $\frac{25866130}{6,07} = 4261,36KB/sec$
Average transfer-rate: $\frac{4004,04+4261,36}{2} = 4132,70KB/sec$
Vectors:
$n4c8 = (100, 100, 70, 90, 50, 55)$
$n4c8e = (100, 100, 70, 90, 50, 55, 4133)$

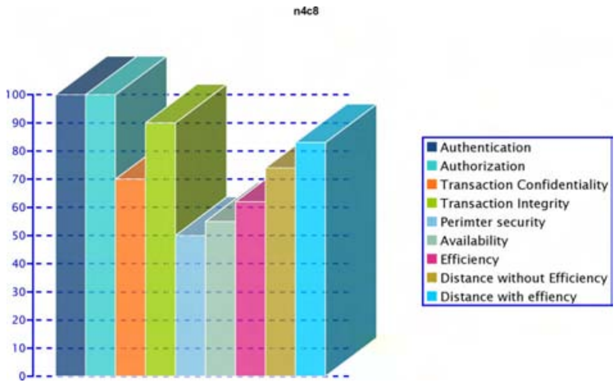

Figure 50: Network 4, measurement 8

4.7.8 Configuration 9

We keep configuration 8. Support for receiving, sending and forwarding messages with integrity protection is removed from the node lcl2.

Transfering between lcl1 and lcl4 with lcl2 and ca as intermediate nodes: Average transfer-rate: $\frac{25866130}{4,22} = 6129,41 KB/sec$
Transfering between lcl1 and lcl4 with lcl3 and ca as intermediate node: Average transfer-rate: $\frac{25866130}{6,07} = 4261,36 KB/sec$
Average transfer-rate: $\frac{6129,41+4261,36}{2} = 5195,39 KB/sec$

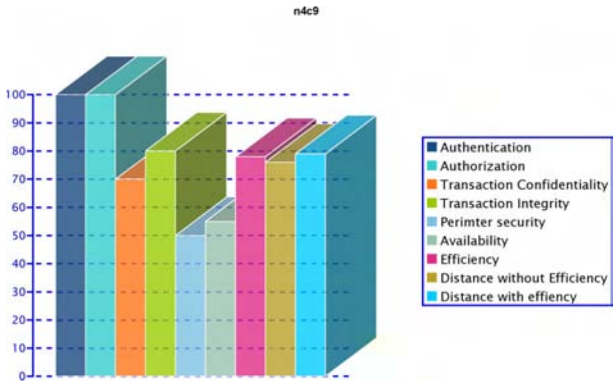

Figure 51: Network 4, measurement 9

Vectors:
$n4c9 = (100, 100, 70, 80, 50, 55)$
$n4c9e = (100, 100, 70, 80, 50, 55, 5195)$

4.7.9 Configuration 10

We keep configuration 9. Support for receiving, sending and forwarding messages with integrity protection is removed from the node lcl3.

Transfering between lcl1 and lcl4 with lcl2 and ca as intermediate nodes: Average transfer-rate: $\frac{25866130}{4,22} = 6129,41 KB/sec$

Transfering between lcl1 and lcl4 with lcl3 and ca as intermediate node: Average transfer-rate: $\frac{25866130}{3,97} = 6515,40KB/sec$
Average transfer-rate: $\frac{6129,41+6515,40}{2} = 6322,41KB/sec$

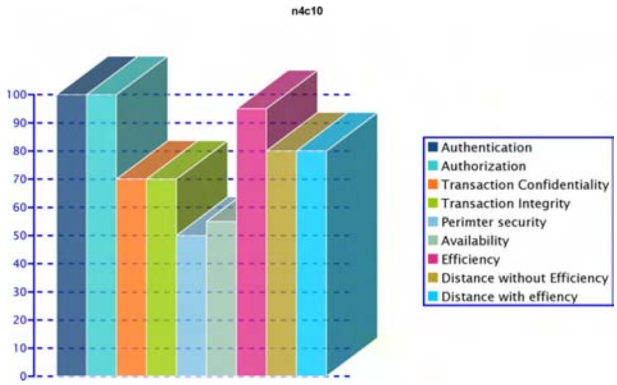

Figure 52: Network 4, measurement 10

Vectors:
$n4c10 = (100, 100, 70, 70, 50, 55)$
$n4c10e = (100, 100, 70, 70, 50, 55, 6322)$

4.8 Results

4.8.1 Summary

This section takes a closer look at the results, by calculating Euclidean distance from the ideal point and classifying the results. The Euclidean distance is calculated to find a comparable number, that tells the distance from the most secure configuration possible. Having this number will make it easier to compare configurations with different numbers of coordinates in the vector, like the vectors with and without efficiency in this case. First of all, the results are listed once more for clarification.

Table 10: Results

n1c1	n1c2	n1c3
(100,100,100,100,50,80)	(100,100,50,100,50,80)	(100,100,50,50,50,80)
n1c4	n1c5	n1c6
(100,100,50,50,50,80)	(100,100,0,50,50,80)	(100,100,0,0,50,80)
n2c1	n2c2	n2c3
(100,100,100,100,50,70)	(100,100,90,100,50,70)	(100,100,90,100,50,70)
n2c4	n2c5	n2c6
(100,100,50,100,50,70)	(100,100,50,90,50,70)	(100,100,50,80,50,70)
n2c7	n2c8	n2c9
(100,100,50,50,50,70)	(100,100,94,94,50,70)	(100,100,88,88,50,70)
n2c10	n2c11	n2c12
(100,100,81,81,50,70)	(100,100,71,81,50,70)	(100,100,61,81,50,70)
n2c13	n2c14	n2c15
(100,100,31,81,50,70)	(100,100,31,71,50,70)	(100,100,31,61,50,70)
n2c16	n3c1	n3c2
(100,100,31,31,50,70)	(100,100,100,100,50,60)	(100,100,90,100,50,60)

n3c3	n3c4	n3c5
(100,100,80,100,50,60)	(100,100,70,100,50,60)	(100,100,70,90,50,60)
n3c6	n3c7	n3c8
(100,100,70,80,50,60)	(100,100,70,70,50,60)	(100,100,92,92,50,60)
n3c9	n3c10	n3c11
(100,100,83,83,50,60)	(100,100,73,83,50,60)	(100,100,63,83,50,60)
n3c12	n3c13	n3c14
(100,100,53,83,50,60)	(100,100,53,73,50,60)	(100,100,53,63,50,60)
n3c15	n4c1	n4c2
(100,100,53,53,50,60)	(100,100,100,100,50,55)	(100,100,80,100,50,55)
n4c3	n4c4	n4c5
(100,100,80,100,50,55)	(100,100,80,90,50,55)	(100,100,80,80,50,55)
n4c6	n4c7	n4c8
(100,100,90,90,50,55)	(100,100,80,90,50,55)	(100,100,70,90,50,55)
n4c9	n4c10	idealp
(100,100,70,90,50,55)	(100,100,70,90,50,55)	(100,100,100,100,100,100)

The vectors with the efficiency included are basically the same, we just have to add the coordinate for the efficiency at the end. When calculating distance from the ideal point, the efficiency coordinate is transformed into a percentage value. Where 100% is the highest transfer rate achieved in this grid (6635250 bytes/sec), and 0% is the same as 0 bytes/sec. From now on, measurements vectors will be referred to according to the measurement numbers, where the vector from the first measurement will be assigned the number one, the vector from the second measurement will be assigned number two and so on. The vectors with efficiency included is treated the same way.

A quick glance at the results reveals the fact that the first coordinate (Authentication), the second coordinate (Authorization), and the fifth coordinate (Perimeter security) never change throughout the process. The first two parameters, authentication and authorization, can be difficult to resolve. This is because the systems in use require authorization, which relies on an authentication scheme. This is also true concerning transferring data with gridFTP.

Next step is to measure the distance from the ideal point to each vector. A direct consequence of this is that the higher each score is, the closer to the ideal point. The distance of a vector from the ideal point might make it easier to compare with other security configurations, and certainly easier to compare the vectors without efficiency to the vectors with efficiency. As mentioned earlier Euclidean distance is used to measure the distance. The following are the results for the vectors without efficiency:

Table 11: Distance results without efficiency

Vector	Distance	Vector	Distance	Vector	Distance
n1c1	54	n4c2	70	n2c6	79
n2c1	58	n4c7	71	n4c10	80
n2c8	59	n4c4	71	n3c12	81
n2c3	59	n3c5	71	n3c13	84
n2c2	59	n3c4	71	n3c14	88

n2c9	61	n3c10	72	n1c4	89
n3c1	64	n4c5	73	n1c3	89
n2c10	64	n3c6	73	n3c15	92
n3c8	65	n2c12	73	n2c13	92
n3c2	65	n1c2	73	n2c7	92
n4c1	67	n4c8	74	n2c14	95
n3c3	67	n4c9	76	n2c15	98
n3c9	68	n3c11	76	n2c16	114
n2c11	68	n3c7	77	n1c5	124
n4c6	69	n2c5	77	n1c6	151
n4c3	70	n2c4	77		

One can clearly see that removing security measures influences the distance a vector has from the ideal point. The difference between vector n1c1 and n2c1 is that 20% of the communication lines are removed from n2c1. As one can see from the distance results, this only affects the distance from the ideal point by 4 points. This is because every coordinate in the vector is weighted equally, and because every aspect of every metric is weighted the same within the metric.

Table 12: Distance results with effiency

Vector	Distance	Vector	Distance	Vector	Distance
n4c9e	79	n3c8e	92	n3c4e	108
n4c10e	80	n1c1e	92	n4c3e	109
n2c12e	82	n2c8e	93	n3c6e	109
n4c8e	83	n2c14e	98	n2c6e	109
n3c10e	83	n2c13e	98	n2c5e	109
n2c11e	83	n2c1e	98	n2c4e	109
n3c11e	84	n1c2e	98	n4c2e	110
n2c10e	84	n2c15e	99	n4c4e	111
n3c13e	85	n2c3e	99	n3c7e	111
n4c7e	86	n2c2e	99	n4c5e	112
n3c14e	88	n1c3e	102	n1c4e	113
n2c9e	88	n3c2e	104	n2c16e	114
n3c12e	89	n3c1e	104	n2c7e	118
n4c6e	90	n3c3e	105	n1c5e	135
n3c9e	90	n3c5e	107	n1c6e	152
n3c15e	92	n4c1e	108		

Both the vectors with efficiency included and vectors without efficiency included have also been classified, using the k-means clustering algorithm. The vectors have been classified into two clusters. Instead of listing the names of each vector in the clusters, the vectors are numbered. The reason for classifying is to see if we can make groups of vectors that are similar to eachother. This is to see if we can find security configurations with the same properties as another security configuration. When the vectors with no efficiency included are clustered we get the following result:

Cluster 1: 1, 2, 7, 8, 9, 10, 11, 12, 14, 15, 16, 17, 18, 23, 24, 25, 26, 27, 28, 29, 31, 32, 33, 34, 38, 39, 40, 41, 42, 43, 44, 45

Cluster 2: 3, 4, 5, 6, 19, 20, 21, 22, 35, 36, 37

The results of clustering the vectors with efficiency included are:

Cluster 1: 1, 2, 4, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 23, 24, 25, 26, 27, 28, 29, 31, 32, 33, 38, 39, 40, 41, 42, 43, 44, 45

Cluster 2: 3, 5, 6, 19, 20, 21, 22, 34, 35, 36, 37, 46, 47

4.8.2 Discussion

Looking at the results, one can see there is differences in the distance to the ideal point. This is true both with and without efficiency included. The differences in the distance from the ideal point might not be as big as one would expect. Looking at the vectors where efficiency is included one notice the vectors are even more alike. This seems to be the result of different security configurations yielding approximately the same distance from the ideal point. Another reason for these similarities in distance from the ideal point is because every measurement criterion has the same weight. When every criterion is weighed equally, each criterion don't affect the result that much on its own.

It is easy to notice that the results from both vectors with and without efficiency included, is quite different. The vectors differ both in the actual distance to the ideal point, and the mutual distance to the ideal point. The vector without efficiency closest to the ideal point is n1c1. This is the vector with most security features implemented, and is logically the most secure vector. Efficiency could be argued to be a part of availability, since for the particular information at hand efficiency is more important than anything else. When the efficiency coordinate is added to n1c1, the new corresponding vector is n1c1e. As we can see, this is not the most secure configuration if efficiency is weighted the same as any of the other security measures. With efficiency included n1c1 is actually only the 18th most secure configuration of all the configurations.

The vector n3c14 is a pretty insecure configuration when efficiency is ignored (37th most secure configuration). When comparing the n3c14e vector, which is n3c14 with efficiency included, to other vectors with efficiency included the score is quite a bit higher (11th most secure configuration when compared to other configurations with efficiency included).

When looking at the vector n3c5 it is the 20th most secure configuration when efficiency is included, and when efficiency is included it is the 31st most secure configuration. This is because this vector is neither secure, unsecure, effective or ineffective.

At first glance the clusters for both vectors with efficiency and vectors without efficiency look quite similar. Taking a closer look reveals the fact that they actually are quite similar. When going from the vectors without efficiency included to the vectors with efficiency included, the first cluster shrink a little bit, and the second cluster grows proportionally. In the clusters with efficiency included, vector 34, 46 and 47 has moved to the second cluster (from the first cluster), and vector 4 has moved to the first cluster (from the second cluster). Low transaction integrity and/or privacy seems to be the factor connecting the vectors in the second cluster when the vectors without efficiency included are considered. When considering the vectors with efficiency included, the second cluster seems to collect the same vectors as in the clustering without efficiency, but now the vectors also got to have an efficiency above some threshold to be a member of the second cluster. Considering this, it looks like the second cluster contains 'less' secure but more efficient configurations.

5 Further work

Weighing is not considered in the metrics presented in this thesis. This can be a weakness in the metric design. As one can see of the results, changing one aspect of one metric hardly affects the result at all. Implementing and testing of these metrics to see how weighing of the the metrics, and even weighing of the metric specific aspects, affects the results. Analysis on how weighing can be used to focus at the specific aspects one feel is important when measuring the security may be useful too.

The fact that 3 of the 6 coordinates in the vectors is unchanged during the measurements, is a weakness that should be addressed in any further work considering the metrics presented. Tests should be run, where all the coordinates are affected by removing security mechanisms. This to get more information from the analysis of the final data, and to see how those 3 coordinates actually affects the final result.

Security concerning the establishment of VOs, and creation of resources is not addressed by the metrics presented. This can be looked upon as a flaw which needs further study, since the joining of VOs and the dynamic creations of resources is what really makes the grid what it is.

6 Conclusion

In this thesis, metrics for measuring security in a GCE are developed. An extensive experimental testing of various GCE configurations has been carried out. The testing shows different results, when different configurations are being tested. This is due to the fact that the different configurations are at different levels when considering security. Another piece of information revealed by the testing is that security and efficiency might not work as well together as one could wish for.

The metrics developed in this thesis measures some aspects of the security in the GCE. This can be derived from the fact that removing security measures increases the distance to the ideal point, which is true for both vectors with and without efficiency included. The metrics developed in this thesis might not suit the need of everyone since these metrics are general. The fact that the metrics are general also leads to only minor distances from ideal point changes, when one feels that a large number of security measures are removed. To make these metrics suit one's needs, one should probably introduce weight to the coordinates, and even to the aspect of each coordinate in order to concentrate on the actual security needed at the site.

Classification of the vectors is possible. In this thesis two clusters were used. The less secure vectors (considering transaction security) ended up in one cluster, while the rest of the vectors ended up in another cluster. With efficiency introduced into these vectors, the classification is still approximately the same. Now the less secure configurations are the most efficient grids. In the measurements results presented in this thesis, the efficiency is weighted the same amount as the rest of the coordinates. If efficiency were a part of the availability metric the vectors wouldn't have differed as much as in this thesis.

Weighting of the security aspects is important, since security seems to affect efficiency quite a bit. One should try to modify as few metrics as possible at the time since more coordinates in the vector would make changes almost invisible in the final distance and classification result.

Bibliography

[1] Ahmar Abbas. *Grid Computing - A Practical Guide to Technology and Applications*. Charles River Media Inc, 2003.

[2] W R Cheswick. S M Bellovin. Firewalls and internet security: Repelling the wily hacker. Technical report, Addison-Wesley, Reading, MA, 1994.

[3] Matt Bishop. *Computer Security - Art and science*. Addison-Wesley, 2nd printing edition, 2003.

[4] Anthony Nadalin IBM. Chris Kaler Microsoft. Phillip Hallam-Baker VeriSign. Ronald Monzillo Sun (Editors). Web services security: Soap message security v1.0. Technical report, IBM, Microsoft, VeriSign, Sun, 2004.

[5] Anthony Nadalin IBM. Chris Kaler Microsoft. Phillip Hallam-Baker VeriSign. Ronald Monzillo Sun (Editors). Web services security: Soap messages with attachments. Technical report, IBM, Microsoft, VeriSign, Sun, 2004.

[6] Anthony Nadalin IBM. Chris Kaler Microsoft. Phillip Hallam-Baker VeriSign. Ronald Monzillo Sun (Editors). Web services security: X.509 token profile v1.0. Technical report, IBM, Microsoft, VeriSign, Sun, 2004.

[7] Fermilab. Strong authentication at fermilab. Technical report, Fermilab, 2004.

[8] Ian Foster and Carl Kesselman. *The Grid: Blueprint for a New Computing Infrastructure*. Morgan Kaufman Publishers, 2nd edition, 2004.

[9] Marianne Swanson. Nadya Bartol. John Sabato. Joan Hash. and Laurie Graffo. Security metrics guide for information technology systems. Technical report, NIST - National Institute of Standards and Technology (U.S. Department of Commerce), 2003.

[10] Carl Kesselman Ian Foster, Nicholas T. Karonis. Managing security in high-performance distributed computations. Technical report, The Globus Alliance http://www.globus.org, 1997.

[11] ISO. Iso 17799: Information technology - code of practice for information security management. Technical report, ISO/IEC, 2000.

[12] A. Jain. Data clustering. *ACM Computing Surveys, Vol 31, No 3, September*, 1999.

[13] Von Welch Jason Novotny, Steven Tuecke. An online credential repository for the grid: Myproxy. Technical report, The Globus Alliance http://www.globus.org, 2001.

[14] Jan Vidar Simonsen Jørgen Belsaas, Sverre Moe. Indikatorer for perimetersikring. Technical report, NISLab - Gjøvik University College, 2004. This article is in norwegian.

[15] Kristof Van Laerhoven. Statistics and metrics for sensor analysis.

[16] Claudia Leopold. *Parallel and Distributed Computing - A Survey of Models paradigms, and Approaches*. John Wiley & Sons Inc, 2001.

[17] B Gleeson. A Lin. J Heinanen. T Finland. G Armitage. A Malis. Ip based virtual private networks. Technical report, Internet Engineering Task Force, RFC 2764, ietf.org/rfc/rfc2764.txt, 1975.

[18] Bob Atkinson Microsoft. Giovanni Della-Libera Microsoft. Satoshi Hada IBM. Maryann Hondo IBM. Phillip Hallam-Baker VeriSign. Johannes Klein Microsoft. Brian LaMacchia Microsoft. Paul Leach Microsoft. John Manferdelli Microsoft. Hiroshi Maruyama IBM. Anthony Nadalin IBM. Nataraj Nagaratnam IBM. Hemma Prafullchandra VeriSign. John Shewchuk Microsoft. Dan Simon Microsoft. Web services security (ws-security). Technical report, IBM, Microsoft, VeriSign, 2002.

[19] Marcin Adamski. Michal Chmielewski. Sergiusz Fonrobert. Adam Gowdiak. Bartosz Lewandowski. Jarek Nabrzyski. Tomasz Ostwald. Juliusz Pukacki. D6.1 requirements document. Technical report, GridLab - http://www.gridlab.org, 2001.

[20] Steinar Lieungh Robert Rinnan, Vegard Wærp. Indikatorer for å karakterisere robusthet på passordbeskyttelse. Technical report, NISLab - Gjøvik University College, 2004.

[21] J. H. Saltzer. The protection of information in computer systems. Technical report, Proceedings of the IEEE, 1975.

[22] V Welch. I Foster. C Kesselman. O Mulmo. L Pearlman. S Tuecke. J Gawor. S Meder. F Siebenlist. X.509 proxy certificates for dynamic delegation. *3rd Annual PKI R&D Workshop*, 2004.

[23] William Stallings. *Network Security Essentials - Applications and Standars*. Prentice Hall, Pearson Education International, 2nd edition, 2003.

[24] Karen Kent Frederick. Ronald W. Ritchey Stephen Northcutt. Lenny Zeltser. Scott Winters. *INSIDE - Network Perimeter Security*. New Riders, 2003.

[25] Ian Foster. Carl Kesselman. Gene Tsudik. Steven Tuecke. A security architecture for computational grids. Technical report, The Globus Alliance http://www.globus.org, 1998.

[26] Ian Foster. Nicholas T Karonis. Carl Kesselman. Greg Koenig. Steven Tuecke. A secure communications infrastructure for high-performance distributed computing. Technical report, The Globus Alliance http://www.globus.org, 1997.

[27] Von Welch. Frank Siebenlist. Ian Foster. John Bresnahan. Karl Czajkowski. Jarek Gawor. Carl Kesselman. Sam Meder. Laura Pearlman. Steven Tuecke. Security for grid services. Technical report, The Globus Alliance http://www.globus.org, 2003.

[28] Ian Foster. Carl Kesselman. Steven Tuecke. Laura Pearlman. Von Welch. A community authorization service for group collaboration. Technical report, The Globus Alliance http://www.globus.org, 2002.

A Measurement results

A.1 Network 1

Table 13: Measurement n1c1

Authentication	Q1	$\frac{5}{5} = 100\%$	$\frac{Q1+Q2+Q3}{3}$
	Q2	$\frac{5}{5} = 100\%$	$= 100\%$
	Q3	$\frac{1}{1} = 100\%$	
Authorization	Q1	$\frac{5}{5} = 100\%$	$\frac{Q1+Q2}{2}$
	Q2	$\frac{5}{5} = 100\%$	$= 100\%$
Transaction confidentiality	Q1	$\frac{10}{10} = 100\%$	$\frac{Q1+Q2}{2}$
	Q2	$\frac{5}{5} = 100\%$	$= 100\%$
Transaction integrity	Q1	$\frac{10}{10} = 100\%$	$\frac{Q1+Q2}{2}$
	Q2	$\frac{5}{5} = 100\%$	$= 100\%$
Perimeter security	Q1	$\frac{0}{0} = 100\%$	$\frac{Q1+Q2+Q3+Q4+Q5+Q6}{6}$
	Q2	$\frac{0}{0} = 100\%$	$= 50\%$
	Q3	$\frac{0}{5} = 0\%$	
	Q4	$\frac{0}{5} = 0\%$	
	Q5	$\frac{10}{10} = 100\%$	
	Q6	$\frac{0}{10} = 0\%$	
Availability	Q1	$\frac{\sum_{n=1}^{5} \frac{(node(n)\ connections)}{4}}{5} = 100\%$	$\frac{Q1+Q2}{2}$
	Q2	$\frac{\sum_{n=1}^{1} \frac{3}{5}}{\#1} = 60\%$	$= 80\%$

Table 14: Measurement n1c2

Authentication	Q1	$\frac{5}{5} = 100\%$	$\frac{Q1+Q2+Q3}{3}$
	Q2	$\frac{5}{5} = 100\%$	$= 100\%$
	Q3	$\frac{1}{1} = 100\%$	
Authorization	Q1	$\frac{5}{5} = 100\%$	$\frac{Q1+Q2}{2}$
	Q2	$\frac{5}{5} = 100\%$	$= 100\%$
Transaction confidentiality	Q1	$\frac{10}{10} = 100\%$	$\frac{Q1+Q2}{2}$
	Q2	$\frac{0}{5} = 0\%$	$= 50\%$
Transaction integrity	Q1	$\frac{10}{10} = 100\%$	$\frac{Q1+Q2}{2}$
	Q2	$\frac{5}{5} = 100\%$	$= 100\%$
Perimeter security	Q1	$\frac{0}{0} = 100\%$	$\frac{Q1+Q2+Q3+Q4+Q5+Q6}{6}$
	Q2	$\frac{0}{0} = 100\%$	$= 50\%$
	Q3	$\frac{0}{5} = 0\%$	
	Q4	$\frac{0}{5} = 0\%$	
	Q5	$\frac{10}{10} = 100\%$	
	Q6	$\frac{0}{10} = 0\%$	
Availability	Q1	$\frac{\sum_{n=1}^{5} \frac{(node(n)\ connections)}{4}}{5} = 100\%$	$\frac{Q1+Q2}{2}$

	Q2	$\frac{\sum_{n=1}^{1} \frac{3}{5}}{\#1} = 60\%$	$= 80\%$

Table 15: Measurement n1c3

Authentication	Q1	$\frac{5}{5} = 100\%$	$\frac{Q1+Q2+Q3}{3}$ $= 100\%$
	Q2	$\frac{5}{5} = 100\%$	
	Q3	$\frac{1}{1} = 100\%$	
Authorization	Q1	$\frac{5}{5} = 100\%$	$\frac{Q1+Q2}{2}$ $= 100\%$
	Q2	$\frac{5}{5} = 100\%$	
Transaction confidentiality	Q1	$\frac{10}{10} = 100\%$	$\frac{Q1+Q2}{2}$ $= 50\%$
	Q2	$\frac{0}{5} = 0\%$	
Transaction integrity	Q1	$\frac{10}{10} = 100\%$	$\frac{Q1+Q2}{2}$ $= 50\%$
	Q2	$\frac{0}{5} = 50\%$	
Perimeter security	Q1	$\frac{0}{0} = 100\%$	$\frac{Q1+Q2+Q3+Q4+Q5+Q6}{6}$ $= 50\%$
	Q2	$\frac{0}{0} = 100\%$	
	Q3	$\frac{0}{5} = 0\%$	
	Q4	$\frac{0}{5} = 0\%$	
	Q5	$\frac{10}{10} = 100\%$	
	Q6	$\frac{0}{10} = 0\%$	
Availability	Q1	$\frac{\sum_{n=1}^{5} \frac{(node(n)\ connections)}{4}}{5} = 100\%$	$\frac{Q1+Q2}{2}$
	Q2	$\frac{\sum_{n=1}^{1} \frac{3}{5}}{\#1} = 60\%$	$= 80\%$

Table 16: Measurement n1c4

Authentication	Q1	$\frac{5}{5} = 100\%$	$\frac{Q1+Q2+Q3}{3}$ $= 100\%$
	Q2	$\frac{5}{5} = 100\%$	
	Q3	$\frac{1}{1} = 100\%$	
Authorization	Q1	$\frac{5}{5} = 100\%$	$\frac{Q1+Q2}{2}$ $= 100\%$
	Q2	$\frac{5}{5} = 100\%$	
Transaction confidentiality	Q1	$\frac{0}{10} = 0\%$	$\frac{Q1+Q2}{2}$ $= 50\%$
	Q2	$\frac{5}{5} = 100\%$	
Transaction integrity	Q1	$\frac{0}{10} = 100\%$	$\frac{Q1+Q2}{2}$ $= 50\%$
	Q2	$\frac{5}{5} = 100\%$	
Perimeter security	Q1	$\frac{0}{0} = 100\%$	$\frac{Q1+Q2+Q3+Q4+Q5+Q6}{6}$ $= 50\%$
	Q2	$\frac{0}{0} = 100\%$	
	Q3	$\frac{0}{5} = 0\%$	
	Q4	$\frac{0}{5} = 0\%$	
	Q5	$\frac{10}{10} = 100\%$	
	Q6	$\frac{0}{10} = 0\%$	
Availability	Q1	$\frac{\sum_{n=1}^{5} \frac{(node(n)\ connections)}{4}}{5} = 100\%$	$\frac{Q1+Q2}{2}$
	Q2	$\frac{\sum_{n=1}^{1} \frac{3}{5}}{\#1} = 60\%$	$= 80\%$

Table 17: Measurement n1c5

Authentication	Q1	$\frac{5}{5} = 100\%$	$\frac{Q1+Q2+Q3}{3} = 100\%$
	Q2	$\frac{5}{5} = 100\%$	
	Q3	$\frac{1}{1} = 100\%$	
Authorization	Q1	$\frac{5}{5} = 100\%$	$\frac{Q1+Q2}{2} = 100\%$
	Q2	$\frac{5}{5} = 100\%$	
Transaction confidentiality	Q1	$\frac{0}{10} = 0\%$	$\frac{Q1+Q2}{2} = 0\%$
	Q2	$\frac{0}{5} = 0\%$	
Transaction integrity	Q1	$\frac{0}{10} = 0\%$	$\frac{Q1+Q2}{2} = 50\%$
	Q2	$\frac{5}{5} = 100\%$	
Perimeter security	Q1	$\frac{0}{0} = 100\%$	$\frac{Q1+Q2+Q3+Q4+Q5+Q6}{6} = 50\%$
	Q2	$\frac{0}{0} = 100\%$	
	Q3	$\frac{0}{5} = 0\%$	
	Q4	$\frac{0}{5} = 0\%$	
	Q5	$\frac{10}{10} = 100\%$	
	Q6	$\frac{0}{10} = 0\%$	
Availability	Q1	$\frac{\sum_{n=1}^{5}\frac{(node(n)\ connections)}{4}}{5} = 100\%$	$\frac{Q1+Q2}{2}$
	Q2	$\frac{\sum_{n=1}^{1}\frac{3}{5}}{\#1} = 60\%$	$= 80\%$

Table 18: Measurement n1c6

Authentication	Q1	$\frac{5}{5} = 100\%$	$\frac{Q1+Q2+Q3}{3} = 100\%$
	Q2	$\frac{5}{5} = 100\%$	
	Q3	$\frac{1}{1} = 100\%$	
Authorization	Q1	$\frac{5}{5} = 100\%$	$\frac{Q1+Q2}{2} = 100\%$
	Q2	$\frac{5}{5} = 100\%$	
Transaction confidentiality	Q1	$\frac{0}{10} = 0\%$	$\frac{Q1+Q2}{2} = 0\%$
	Q2	$\frac{0}{5} = 0\%$	
Transaction integrity	Q1	$\frac{0}{10} = 0\%$	$\frac{Q1+Q2}{2} = 0\%$
	Q2	$\frac{0}{5} = 0\%$	
Perimeter security	Q1	$\frac{0}{0} = 100\%$	$\frac{Q1+Q2+Q3+Q4+Q5+Q6}{6} = 50\%$
	Q2	$\frac{0}{0} = 100\%$	
	Q3	$\frac{0}{5} = 0\%$	
	Q4	$\frac{0}{5} = 0\%$	
	Q5	$\frac{10}{10} = 100\%$	
	Q6	$\frac{0}{10} = 0\%$	
Availability	Q1	$\frac{\sum_{n=1}^{5}\frac{(node(n)\ connections)}{4}}{5} = 100\%$	$\frac{Q1+Q2}{2}$
	Q2	$\frac{\sum_{n=1}^{1}\frac{3}{5}}{\#1} = 60\%$	$= 80\%$

A.2 Network 2

Table 19: Measurement n2c1

Authentication	Q1	$\frac{5}{5} = 100\%$	$\frac{Q1+Q2+Q3}{3}$
	Q2	$\frac{5}{5} = 100\%$	$= 100\%$
	Q3	$\frac{1}{1} = 100\%$	
Authorization	Q1	$\frac{5}{5} = 100\%$	$\frac{Q1+Q2}{2}$ $= 100\%$
	Q2	$\frac{5}{5} = 100\%$	
Transaction confidentiality	Q1	$\frac{8}{8} = 100\%$	$\frac{Q1+Q2}{2}$ $= 100\%$
	Q2	$\frac{5}{5} = 100\%$	
Transaction integrity	Q1	$\frac{8}{8} = 100\%$	$\frac{Q1+Q2}{2}$ $= 100\%$
	Q2	$\frac{8}{8} = 100\%$	
Perimeter security	Q1	$\frac{0}{0} = 100\%$	$\frac{Q1+Q2+Q3+Q4+Q5+Q6}{6}$ $= 50\%$
	Q2	$\frac{0}{0} = 100\%$	
	Q3	$\frac{0}{5} = 0\%$	
	Q4	$\frac{0}{5} = 0\%$	
	Q5	$\frac{8}{8} = 100\%$	
	Q6	$\frac{0}{8} = 0\%$	
Availability	Q1	$\frac{\sum_{n=1}^{5} \frac{(node(n)\ connections)}{4}}{5} = 80\%$	$\frac{Q1+Q2}{2}$ $= 70\%$
	Q2	$\frac{\sum_{n=1}^{1} \frac{3}{5}}{\#1} = 60\%$	

Table 20: Measurement n2c2

Authentication	Q1	$\frac{5}{5} = 100\%$	$\frac{Q1+Q2+Q3}{3}$ $= 100\%$
	Q2	$\frac{5}{5} = 100\%$	
	Q3	$\frac{1}{1} = 100\%$	
Authorization	Q1	$\frac{5}{5} = 100\%$	$\frac{Q1+Q2}{2}$ $= 100\%$
	Q2	$\frac{5}{5} = 100\%$	
Transaction confidentiality	Q1	$\frac{8}{8} = 100\%$	$\frac{Q1+Q2}{2}$ $= 90\%$
	Q2	$\frac{4}{5} = 80\%$	
Transaction integrity	Q1	$\frac{8}{8} = 100\%$	$\frac{Q1+Q2}{2}$ $= 100\%$
	Q2	$\frac{5}{5} = 100\%$	
Perimeter security	Q1	$\frac{0}{0} = 100\%$	$\frac{Q1+Q2+Q3+Q4+Q5+Q6}{6}$ $= 50\%$
	Q2	$\frac{0}{0} = 100\%$	
	Q3	$\frac{0}{5} = 0\%$	
	Q4	$\frac{0}{5} = 0\%$	
	Q5	$\frac{8}{8} = 100\%$	
	Q6	$\frac{0}{8} = 0\%$	
Availability	Q1	$\frac{\sum_{n=1}^{5} \frac{(node(n)\ connections)}{4}}{5} = 80\%$	$\frac{Q1+Q2}{2}$ $= 70\%$
	Q2	$\frac{\sum_{n=1}^{1} \frac{3}{5}}{\#1} = 60\%$	

Table 21: Measurement n2c3

Authentication	Q1	$\frac{5}{5} = 100\%$	$\frac{Q1+Q2+Q3}{3}$
	Q2	$\frac{5}{5} = 100\%$	$= 100\%$
	Q3	$\frac{1}{1} = 100\%$	
Authorization	Q1	$\frac{5}{5} = 100\%$	$\frac{Q1+Q2}{2}$
	Q2	$\frac{5}{5} = 100\%$	$= 100\%$
Transaction confidentiality	Q1	$\frac{8}{8} = 100\%$	$\frac{Q1+Q2}{2}$
	Q2	$\frac{3}{5} = 0\%$	$= 50\%$
Transaction integrity	Q1	$\frac{8}{8} = 100\%$	$\frac{Q1+Q2}{2}$
	Q2	$\frac{5}{5} = 100\%$	$= 100\%$
Perimeter security	Q1	$\frac{0}{0} = 100\%$	$\frac{Q1+Q2+Q3+Q4+Q5+Q6}{6}$
	Q2	$\frac{0}{0} = 100\%$	$= 50\%$
	Q3	$\frac{0}{5} = 0\%$	
	Q4	$\frac{0}{5} = 0\%$	
	Q5	$\frac{8}{8} = 100\%$	
	Q6	$\frac{0}{8} = 0\%$	
Availability	Q1	$\frac{\sum_{n=1}^{5} \frac{(node(n)\ connections)}{4}}{5} = 80\%$	$\frac{Q1+Q2}{2}$
	Q2	$\frac{\sum_{n=1}^{1} \frac{3}{5}}{\#1} = 60\%$	$= 70\%$

Table 22: Measurement n2c4

Authentication	Q1	$\frac{5}{5} = 100\%$	$\frac{Q1+Q2+Q3}{3}$
	Q2	$\frac{5}{5} = 100\%$	$= 100\%$
	Q3	$\frac{1}{1} = 100\%$	
Authorization	Q1	$\frac{5}{5} = 100\%$	$\frac{Q1+Q2}{2}$
	Q2	$\frac{5}{5} = 100\%$	$= 100\%$
Transaction confidentiality	Q1	$\frac{8}{8} = 100\%$	$\frac{Q1+Q2}{2}$
	Q2	$\frac{0}{5} = 0\%$	$= 50\%$
Transaction integrity	Q1	$\frac{8}{8} = 100\%$	$\frac{Q1+Q2}{2}$
	Q2	$\frac{5}{5} = 100\%$	$= 100\%$
Perimeter security	Q1	$\frac{0}{0} = 100\%$	$\frac{Q1+Q2+Q3+Q4+Q5+Q6}{6}$
	Q2	$\frac{0}{0} = 100\%$	$= 50\%$
	Q3	$\frac{0}{5} = 0\%$	
	Q4	$\frac{0}{5} = 0\%$	
	Q5	$\frac{8}{8} = 100\%$	
	Q6	$\frac{0}{8} = 0\%$	
Availability	Q1	$\frac{\sum_{n=1}^{5} \frac{(node(n)\ connections)}{4}}{5} = 80\%$	$\frac{Q1+Q2}{2}$
	Q2	$\frac{\sum_{n=1}^{1} \frac{3}{5}}{\#1} = 60\%$	$= 70\%$

Table 23: Measurement n2c5

Authentication	Q1	$\frac{5}{5} = 100\%$	$\frac{Q1+Q2+Q3}{3}$

	Q2	$\frac{5}{5} = 100\%$	$= 100\%$
	Q3	$\frac{1}{1} = 100\%$	
Authorization	Q1	$\frac{5}{5} = 100\%$	$\frac{Q1+Q2}{2}$
	Q2	$\frac{5}{5} = 100\%$	$= 100\%$
Transaction confidentiality	Q1	$\frac{8}{8} = 100\%$	$\frac{Q1+Q2}{2}$
	Q2	$\frac{0}{5} = 0\%$	$= 50\%$
Transaction integrity	Q1	$\frac{8}{8} = 100\%$	$\frac{Q1+Q2}{2}$
	Q2	$\frac{4}{5} = 80\%$	$= 90\%$
Perimeter security	Q1	$\frac{0}{0} = 100\%$	$\frac{Q1+Q2+Q3+Q4+Q5+Q6}{6}$
	Q2	$\frac{0}{0} = 100\%$	$= 50\%$
	Q3	$\frac{0}{5} = 0\%$	
	Q4	$\frac{0}{5} = 0\%$	
	Q5	$\frac{8}{8} = 100\%$	
	Q6	$\frac{0}{8} = 0\%$	
Availability	Q1	$\frac{\sum_{n=1}^{5} \frac{(node(n)\ connections)}{4}}{5} = 80\%$	$\frac{Q1+Q2}{2}$
	Q2	$\frac{\sum_{n=1}^{1} \frac{3}{5}}{\#1} = 60\%$	$= 70\%$

Table 24: Measurement n2c6

Authentication	Q1	$\frac{5}{5} = 100\%$	$\frac{Q1+Q2+Q3}{3}$
	Q2	$\frac{5}{5} = 100\%$	$= 100\%$
	Q3	$\frac{1}{1} = 100\%$	
Authorization	Q1	$\frac{5}{5} = 100\%$	$\frac{Q1+Q2}{2}$
	Q2	$\frac{5}{5} = 100\%$	$= 100\%$
Transaction confidentiality	Q1	$\frac{8}{8} = 100\%$	$\frac{Q1+Q2}{2}$
	Q2	$\frac{0}{5} = 0\%$	$= 50\%$
Transaction integrity	Q1	$\frac{8}{8} = 100\%$	$\frac{Q1+Q2}{2}$
	Q2	$\frac{3}{5} = 60\%$	$= 80\%$
Perimeter security	Q1	$\frac{0}{0} = 100\%$	$\frac{Q1+Q2+Q3+Q4+Q5+Q6}{6}$
	Q2	$\frac{0}{0} = 100\%$	$= 50\%$
	Q3	$\frac{0}{5} = 0\%$	
	Q4	$\frac{0}{5} = 0\%$	
	Q5	$\frac{8}{8} = 100\%$	
	Q6	$\frac{0}{8} = 0\%$	
Availability	Q1	$\frac{\sum_{n=1}^{5} \frac{(node(n)\ connections)}{4}}{5} = 80\%$	$\frac{Q1+Q2}{2}$
Availability	Q2	$\frac{\sum_{n=1}^{1} \frac{3}{5}}{\#1} = 60\%$	$= 70\%$

Table 26: Measurement n2c8

Authentication	Q1	$\frac{5}{5} = 100\%$	$\frac{Q1+Q2+Q3}{3}$
	Q2	$\frac{5}{5} = 100\%$	$= 100\%$
	Q3	$\frac{1}{1} = 100\%$	

Authorization	Q1	$\frac{5}{5} = 100\%$	$\frac{Q1+Q2}{2}$ $= 100\%$
	Q2	$\frac{5}{5} = 100\%$	
Transaction confidentiality	Q1	$\frac{7}{8} = 87,5\%$	$\frac{Q1+Q2}{2}$ $= 93,75\%$
	Q2	$\frac{5}{5} = 100\%$	
Transaction integrity	Q1	$\frac{7}{8} = 87,5\%$	$\frac{Q1+Q2}{2}$ $= 93,75\%$
	Q2	$\frac{5}{5} = 100\%$	
Perimeter security	Q1	$\frac{0}{0} = 100\%$	$\frac{Q1+Q2+Q3+Q4+Q5+Q6}{6}$ $= 50\%$
	Q2	$\frac{0}{0} = 100\%$	
	Q3	$\frac{0}{5} = 0\%$	
	Q4	$\frac{0}{5} = 0\%$	
	Q5	$\frac{8}{8} = 100\%$	
	Q6	$\frac{0}{8} = 0\%$	
Availability	Q1	$\sum_{n=1}^{5} \frac{\frac{(node(n)\ connections)}{4}}{5} = 80\%$	$\frac{Q1+Q2}{2}$ $= 70\%$
	Q2	$\frac{\sum_{n=1}^{1} \frac{3}{5}}{\#1} = 60\%$	

Table 27: Measurement n2c9

Authentication	Q1	$\frac{5}{5} = 100\%$	$\frac{Q1+Q2+Q3}{3}$ $= 100\%$
	Q2	$\frac{5}{5} = 100\%$	
	Q3	$\frac{1}{1} = 100\%$	
Authorization	Q1	$\frac{5}{5} = 100\%$	$\frac{Q1+Q2}{2}$ $= 100\%$
	Q2	$\frac{5}{5} = 100\%$	
Transaction confidentiality	Q1	$\frac{6}{8} = 75\%$	$\frac{Q1+Q2}{2}$ $= 87,5\%$
	Q2	$\frac{5}{5} = 100\%$	
Transaction integrity	Q1	$\frac{6}{8} = 75\%$	$\frac{Q1+Q2}{2}$ $= 87,5\%$
	Q2	$\frac{5}{5} = 100\%$	
Perimeter security	Q1	$\frac{0}{0} = 100\%$	$\frac{Q1+Q2+Q3+Q4+Q5+Q6}{6}$ $= 50\%$
	Q2	$\frac{0}{0} = 100\%$	
	Q3	$\frac{0}{5} = 0\%$	
	Q4	$\frac{0}{5} = 0\%$	
	Q5	$\frac{8}{8} = 100\%$	
	Q6	$\frac{0}{8} = 0\%$	
Availability	Q1	$\sum_{n=1}^{5} \frac{\frac{(node(n)\ connections)}{4}}{5} = 80\%$	$\frac{Q1+Q2}{2}$ $= 70\%$
	Q2	$\frac{\sum_{n=1}^{1} \frac{3}{5}}{\#1} = 60\%$	

Table 28: Measurement n2c10

Authentication	Q1	$\frac{5}{5} = 100\%$	$\frac{Q1+Q2+Q3}{3}$ $= 100\%$
	Q2	$\frac{5}{5} = 100\%$	
	Q3	$\frac{1}{1} = 100\%$	
Authorization	Q1	$\frac{5}{5} = 100\%$	$\frac{Q1+Q2}{2}$ $= 100\%$
	Q2	$\frac{5}{5} = 100\%$	

Transaction confidentiality	Q1	$\frac{5}{8} = 62,5\%$	$\frac{Q1+Q2}{2}$
	Q2	$\frac{5}{5} = 100\%$	$= 81,25\%$
Transaction integrity	Q1	$\frac{5}{8} = 62,5\%$	$\frac{Q1+Q2}{2}$
	Q2	$\frac{5}{5} = 100\%$	$= 81,25\%$
Perimeter security	Q1	$\frac{0}{0} = 100\%$	$\frac{Q1+Q2+Q3+Q4+Q5+Q6}{6}$
	Q2	$\frac{0}{0} = 100\%$	$= 50\%$
	Q3	$\frac{0}{5} = 0\%$	
	Q4	$\frac{0}{5} = 0\%$	
	Q5	$\frac{8}{8} = 100\%$	
	Q6	$\frac{0}{8} = 0\%$	
Availability	Q1	$\frac{\sum_{n=1}^{5} \frac{(node(n)\ connections)}{4}}{5} = 80\%$	$\frac{Q1+Q2}{2}$
	Q2	$\frac{\sum_{n=1}^{1} \frac{3}{5}}{\#1} = 60\%$	$= 70\%$

Table 29: Measurement n2c11

Authentication	Q1	$\frac{5}{5} = 100\%$	$\frac{Q1+Q2+Q3}{3}$
	Q2	$\frac{5}{5} = 100\%$	$= 100\%$
	Q3	$\frac{1}{1} = 100\%$	
Authorization	Q1	$\frac{5}{5} = 100\%$	$\frac{Q1+Q2}{2}$
	Q2	$\frac{5}{5} = 100\%$	$= 100\%$
Transaction confidentiality	Q1	$\frac{5}{8} = 62,5\%$	$\frac{Q1+Q2}{2}$
	Q2	$\frac{4}{5} = 80\%$	$= 71,25\%$
Transaction integrity	Q1	$\frac{5}{8} = 62,5\%$	$\frac{Q1+Q2}{2}$
	Q2	$\frac{5}{5} = 100\%$	$= 81,25\%$
Perimeter security	Q1	$\frac{0}{0} = 100\%$	$\frac{Q1+Q2+Q3+Q4+Q5+Q6}{6}$
	Q2	$\frac{0}{0} = 100\%$	$= 50\%$
	Q3	$\frac{0}{5} = 0\%$	
	Q4	$\frac{0}{5} = 0\%$	
	Q5	$\frac{8}{8} = 100\%$	
	Q6	$\frac{0}{8} = 0\%$	
Availability	Q1	$\frac{\sum_{n=1}^{5} \frac{(node(n)\ connections)}{4}}{5} = 80\%$	$\frac{Q1+Q2}{2}$
	Q2	$\frac{\sum_{n=1}^{1} \frac{3}{5}}{\#1} = 60\%$	$= 70\%$

Table 30: Measurement n2c12

Authentication	Q1	$\frac{5}{5} = 100\%$	$\frac{Q1+Q2+Q3}{3}$
	Q2	$\frac{5}{5} = 100\%$	$= 100\%$
	Q3	$\frac{1}{1} = 100\%$	
Authorization	Q1	$\frac{5}{5} = 100\%$	$\frac{Q1+Q2}{2}$
	Q2	$\frac{5}{5} = 100\%$	$= 100\%$
Transaction confidentiality	Q1	$\frac{5}{8} = 62,5\%$	$\frac{Q1+Q2}{2}$
	Q2	$\frac{3}{5} = 60\%$	$= 61,25\%$

Transaction integrity	Q1	$\frac{5}{8} = 62,5\%$	$\frac{Q1+Q2}{2} = 81,25\%$
	Q2	$\frac{5}{5} = 100\%$	
Perimeter security	Q1	$\frac{0}{0} = 100\%$	$\frac{Q1+Q2+Q3+Q4+Q5+Q6}{6} = 50\%$
	Q2	$\frac{0}{0} = 100\%$	
	Q3	$\frac{0}{5} = 0\%$	
	Q4	$\frac{0}{5} = 0\%$	
	Q5	$\frac{8}{8} = 100\%$	
	Q6	$\frac{0}{8} = 0\%$	
Availability	Q1	$\frac{\sum_{n=1}^{5}\frac{(node(n)\ connections)}{4}}{5} = 80\%$	$\frac{Q1+Q2}{2} = 70\%$
	Q2	$\frac{\sum_{n=1}^{1}\frac{3}{5}}{\#1} = 60\%$	

Table 31: Measurement n2c13

Authentication	Q1	$\frac{5}{5} = 100\%$	$\frac{Q1+Q2+Q3}{3} = 100\%$
	Q2	$\frac{5}{5} = 100\%$	
	Q3	$\frac{1}{1} = 100\%$	
Authorization	Q1	$\frac{5}{5} = 100\%$	$\frac{Q1+Q2}{2} = 100\%$
	Q2	$\frac{5}{5} = 100\%$	
Transaction confidentiality	Q1	$\frac{5}{8} = 62,5\%$	$\frac{Q1+Q2}{2} = 31,25\%$
	Q2	$\frac{0}{5} = 0\%$	
Transaction integrity	Q1	$\frac{5}{8} = 62,5\%$	$\frac{Q1+Q2}{2} = 81,25\%$
	Q2	$\frac{5}{5} = 100\%$	
Perimeter security	Q1	$\frac{0}{0} = 100\%$	$\frac{Q1+Q2+Q3+Q4+Q5+Q6}{6} = 50\%$
	Q2	$\frac{0}{0} = 100\%$	
	Q3	$\frac{0}{5} = 0\%$	
	Q4	$\frac{0}{5} = 0\%$	
	Q5	$\frac{8}{8} = 100\%$	
	Q6	$\frac{0}{8} = 0\%$	
Availability	Q1	$\frac{\sum_{n=1}^{5}\frac{(node(n)\ connections)}{4}}{5} = 80\%$	$\frac{Q1+Q2}{2} = 70\%$
	Q2	$\frac{\sum_{n=1}^{1}\frac{3}{5}}{\#1} = 60\%$	

Table 32: Measurement n2c14

Authentication	Q1	$\frac{5}{5} = 100\%$	$\frac{Q1+Q2+Q3}{3} = 100\%$
	Q2	$\frac{5}{5} = 100\%$	
	Q3	$\frac{1}{1} = 100\%$	
Authorization	Q1	$\frac{5}{5} = 100\%$	$\frac{Q1+Q2}{2} = 100\%$
	Q2	$\frac{5}{5} = 100\%$	
Transaction confidentiality	Q1	$\frac{5}{8} = 62,5\%$	$\frac{Q1+Q2}{2} = 31,25\%$
	Q2	$\frac{0}{5} = 0\%$	
Transaction integrity	Q1	$\frac{5}{8} = 62,5\%$	$\frac{Q1+Q2}{2} = 71,25\%$
	Q2	$\frac{4}{5} = 80\%$	

Perimeter security	Q1	$\frac{0}{0} = 100\%$	$\frac{Q1+Q2+Q3+Q4+Q5+Q6}{6}$
	Q2	$\frac{0}{0} = 100\%$	$= 50\%$
	Q3	$\frac{0}{5} = 0\%$	
	Q4	$\frac{0}{5} = 0\%$	
	Q5	$\frac{8}{8} = 100\%$	
	Q6	$\frac{0}{8} = 0\%$	
Availability	Q1	$\frac{\sum_{n=1}^{5}\frac{(node(n)\ connections)}{4}}{5} = 80\%$	$\frac{Q1+Q2}{2}$
	Q2	$\frac{\sum_{n=1}^{1}\frac{3}{5}}{\#1} = 60\%$	$= 70\%$

Table 33: Measurement n2c15

Authentication	Q1	$\frac{5}{5} = 100\%$	$\frac{Q1+Q2+Q3}{3}$
	Q2	$\frac{5}{5} = 100\%$	$= 100\%$
	Q3	$\frac{1}{1} = 100\%$	
Authorization	Q1	$\frac{5}{5} = 100\%$	$\frac{Q1+Q2}{2}$
	Q2	$\frac{5}{5} = 100\%$	$= 100\%$
Transaction confidentiality	Q1	$\frac{5}{8} = 62,5\%$	$\frac{Q1+Q2}{2}$
	Q2	$\frac{0}{5} = 0\%$	$= 31,25\%$
Transaction integrity	Q1	$\frac{5}{8} = 62,5\%$	$\frac{Q1+Q2}{2}$
	Q2	$\frac{3}{5} = 60\%$	$= 61,25\%$
Perimeter security	Q1	$\frac{0}{0} = 100\%$	$\frac{Q1+Q2+Q3+Q4+Q5+Q6}{6}$
	Q2	$\frac{0}{0} = 100\%$	$= 50\%$
	Q3	$\frac{0}{5} = 0\%$	
	Q4	$\frac{0}{5} = 0\%$	
	Q5	$\frac{8}{8} = 100\%$	
	Q6	$\frac{0}{8} = 0\%$	
Availability	Q1	$\frac{\sum_{n=1}^{5}\frac{(node(n)\ connections)}{4}}{5} = 80\%$	$\frac{Q1+Q2}{2}$
	Q2	$\frac{\sum_{n=1}^{1}\frac{3}{5}}{\#1} = 60\%$	$= 70\%$

Table 34: Measurement n2c16

Authentication	Q1	$\frac{5}{5} = 100\%$	$\frac{Q1+Q2+Q3}{3}$
	Q2	$\frac{5}{5} = 100\%$	$= 100\%$
	Q3	$\frac{1}{1} = 100\%$	
Authorization	Q1	$\frac{5}{5} = 100\%$	$\frac{Q1+Q2}{2}$
	Q2	$\frac{5}{5} = 100\%$	$= 100\%$
Transaction confidentiality	Q1	$\frac{5}{8} = 100\%$	$\frac{Q1+Q2}{2}$
	Q2	$\frac{0}{5} = 100\%$	$= 31,25\%$
Transaction integrity	Q1	$\frac{5}{8} = 100\%$	$\frac{Q1+Q2}{2}$
	Q2	$\frac{0}{5} = 0\%$	$= 31,25\%$
Perimeter security	Q1	$\frac{0}{0} = 100\%$	$\frac{Q1+Q2+Q3+Q4+Q5+Q6}{6}$
	Q2	$\frac{0}{0} = 100\%$	$= 50\%$

	Q3	$\frac{0}{5} = 0\%$	
	Q4	$\frac{0}{5} = 0\%$	
	Q5	$\frac{8}{8} = 100\%$	
	Q6	$\frac{0}{8} = 0\%$	
Availability	Q1	$\frac{\sum_{n=1}^{5} \frac{(node(n)\ connections)}{4}}{5} = 80\%$	$\frac{Q1+Q2}{2}$
	Q2	$\frac{\sum_{n=1}^{1} \frac{3}{5}}{\#1} = 60\%$	$= 70\%$

A.3 Network 3

Table 35: Measurement n3c1

Authentication	Q1	$\frac{5}{5} = 100\%$	$\frac{Q1+Q2+Q3}{3}$
	Q2	$\frac{5}{5} = 100\%$	$= 100\%$
	Q3	$\frac{1}{1} = 100\%$	
Authorization	Q1	$\frac{5}{5} = 100\%$	$\frac{Q1+Q2}{2}$
	Q2	$\frac{5}{5} = 100\%$	$= 100\%$
Transaction confidentiality	Q1	$\frac{6}{6} = 100\%$	$\frac{Q1+Q2}{2}$
	Q2	$\frac{5}{5} = 100\%$	$= 100\%$
Transaction integrity	Q1	$\frac{6}{6} = 100\%$	$\frac{Q1+Q2}{2}$
	Q2	$\frac{5}{5} = 100\%$	$= 100\%$
Perimeter security	Q1	$\frac{0}{0} = 100\%$	$\frac{Q1+Q2+Q3+Q4+Q5+Q6}{6}$
	Q2	$\frac{0}{0} = 100\%$	$= 50\%$
	Q3	$\frac{0}{5} = 0\%$	
	Q4	$\frac{0}{5} = 0\%$	
	Q5	$\frac{6}{6} = 100\%$	
	Q6	$\frac{0}{8} = 0\%$	
Availability	Q1	$\frac{\sum_{n=1}^{5} \frac{(node(n)\ connections)}{4}}{5} = 60\%$	$\frac{Q1+Q2}{2}$
	Q2	$\frac{\sum_{n=1}^{1} \frac{3}{5}}{\#1} = 60\%$	$= 60\%$

Table 36: Measurement n3c2

Authentication	Q1	$\frac{5}{5} = 100\%$	$\frac{Q1+Q2+Q3}{3}$
	Q2	$\frac{5}{5} = 100\%$	$= 100\%$
	Q3	$\frac{1}{1} = 100\%$	
Authorization	Q1	$\frac{5}{5} = 100\%$	$\frac{Q1+Q2}{2}$
	Q2	$\frac{5}{5} = 100\%$	$= 100\%$
Transaction confidentiality	Q1	$\frac{6}{6} = 100\%$	$\frac{Q1+Q2}{2}$
	Q2	$\frac{4}{5} = 80\%$	$= 90\%$
Transaction integrity	Q1	$\frac{6}{6} = 100\%$	$\frac{Q1+Q2}{2}$
	Q2	$\frac{5}{5} = 100\%$	$= 100\%$
Perimeter security	Q1	$\frac{0}{0} = 100\%$	$\frac{Q1+Q2+Q3+Q4+Q5+Q6}{6}$
	Q2	$\frac{0}{0} = 100\%$	$= 50\%$
	Q3	$\frac{0}{5} = 0\%$	
	Q4	$\frac{0}{5} = 0\%$	

	Q5	$\frac{6}{6} = 100\%$	
	Q6	$\frac{0}{8} = 0\%$	
Availability	Q1	$\frac{\sum_{n=1}^{5} \frac{(node(n)\ connections)}{4}}{5} = 60\%$	$\frac{Q1+Q2}{2}$ $= 60\%$
	Q2	$\frac{\sum_{n=1}^{1} \frac{3}{5}}{\#1} = 60\%$	

Table 37: Measurement n3c3

Authentication	Q1	$\frac{5}{5} = 100\%$	$\frac{Q1+Q2+Q3}{3}$ $= 100\%$
	Q2	$\frac{5}{5} = 100\%$	
	Q3	$\frac{1}{1} = 100\%$	
Authorization	Q1	$\frac{5}{5} = 100\%$	$\frac{Q1+Q2}{2}$ $= 100\%$
	Q2	$\frac{5}{5} = 100\%$	
Transaction confidentiality	Q1	$\frac{6}{6} = 100\%$	$\frac{Q1+Q2}{2}$ $= 80\%$
	Q2	$\frac{3}{5} = 60\%$	
Transaction integrity	Q1	$\frac{6}{6} = 100\%$	$\frac{Q1+Q2}{2}$ $= 100\%$
	Q2	$\frac{5}{5} = 100\%$	
Perimeter security	Q1	$\frac{0}{0} = 100\%$	$\frac{Q1+Q2+Q3+Q4+Q5+Q6}{6}$ $= 50\%$
	Q2	$\frac{0}{0} = 100\%$	
	Q3	$\frac{0}{5} = 0\%$	
	Q4	$\frac{0}{5} = 0\%$	
	Q5	$\frac{6}{6} = 100\%$	
	Q6	$\frac{0}{8} = 0\%$	
Availability	Q1	$\frac{\sum_{n=1}^{5} \frac{(node(n)\ connections)}{4}}{5} = 60\%$	$\frac{Q1+Q2}{2}$ $= 60\%$
	Q2	$\frac{\sum_{n=1}^{1} \frac{3}{5}}{\#1} = 60\%$	

Table 38: Measurement n3c4

Authentication	Q1	$\frac{5}{5} = 100\%$	$\frac{Q1+Q2+Q3}{3}$ $= 100\%$
	Q2	$\frac{5}{5} = 100\%$	
	Q3	$\frac{1}{1} = 100\%$	
Authorization	Q1	$\frac{5}{5} = 100\%$	$\frac{Q1+Q2}{2}$ $= 100\%$
	Q2	$\frac{5}{5} = 100\%$	
Transaction confidentiality	Q1	$\frac{6}{6} = 100\%$	$\frac{Q1+Q2}{2}$ $= 70\%$
	Q2	$\frac{2}{5} = 40\%$	
Transaction integrity	Q1	$\frac{6}{6} = 100\%$	$\frac{Q1+Q2}{2}$ $= 100\%$
	Q2	$\frac{5}{5} = 100\%$	
Perimeter security	Q1	$\frac{0}{0} = 100\%$	$\frac{Q1+Q2+Q3+Q4+Q5+Q6}{6}$ $= 50\%$
	Q2	$\frac{0}{0} = 100\%$	
	Q3	$\frac{0}{5} = 0\%$	
	Q4	$\frac{0}{5} = 0\%$	
	Q5	$\frac{6}{6} = 100\%$	
	Q6	$\frac{0}{8} = 0\%$	

Availability	Q1	$\sum_{n=1}^{5} \frac{\frac{(node(n)\ connections)}{4}}{5} = 60\%$	$\frac{Q1+Q2}{2}$ $= 60\%$
	Q2	$\frac{\sum_{n=1}^{1} \frac{3}{5}}{\#1} = 60\%$	

Table 39: Measurement n3c5

Authentication	Q1	$\frac{5}{5} = 100\%$	$\frac{Q1+Q2+Q3}{3}$ $= 100\%$
	Q2	$\frac{5}{5} = 100\%$	
	Q3	$\frac{1}{1} = 100\%$	
Authorization	Q1	$\frac{5}{5} = 100\%$	$\frac{Q1+Q2}{2}$ $= 100\%$
	Q2	$\frac{5}{5} = 100\%$	
Transaction confidentiality	Q1	$\frac{6}{6} = 100\%$	$\frac{Q1+Q2}{2}$ $= 70\%$
	Q2	$\frac{2}{5} = 40\%$	
Transaction integrity	Q1	$\frac{6}{6} = 100\%$	$\frac{Q1+Q2}{2}$ $= 90\%$
	Q2	$\frac{4}{5} = 80\%$	
Perimeter security	Q1	$\frac{0}{0} = 100\%$	$\frac{Q1+Q2+Q3+Q4+Q5+Q6}{6}$ $= 50\%$
	Q2	$\frac{0}{0} = 100\%$	
	Q3	$\frac{0}{5} = 0\%$	
	Q4	$\frac{0}{5} = 0\%$	
	Q5	$\frac{6}{6} = 100\%$	
	Q6	$\frac{0}{8} = 0\%$	
Availability	Q1	$\sum_{n=1}^{5} \frac{\frac{(node(n)\ connections)}{4}}{5} = 60\%$	$\frac{Q1+Q2}{2}$ $= 60\%$
	Q2	$\frac{\sum_{n=1}^{1} \frac{3}{5}}{\#1} = 60\%$	

Table 40: Measurement n3c6

Authentication	Q1	$\frac{5}{5} = 100\%$	$\frac{Q1+Q2+Q3}{3}$ $= 100\%$
	Q2	$\frac{5}{5} = 100\%$	
	Q3	$\frac{1}{1} = 100\%$	
Authorization	Q1	$\frac{5}{5} = 100\%$	$\frac{Q1+Q2}{2}$ $= 100\%$
	Q2	$\frac{5}{5} = 100\%$	
Transaction confidentiality	Q1	$\frac{6}{6} = 100\%$	$\frac{Q1+Q2}{2}$ $= 70\%$
	Q2	$\frac{2}{5} = 40\%$	
Transaction integrity	Q1	$\frac{6}{6} = 100\%$	$\frac{Q1+Q2}{2}$ $= 80\%$
	Q2	$\frac{3}{5} = 60\%$	
Perimeter security	Q1	$\frac{0}{0} = 100\%$	$\frac{Q1+Q2+Q3+Q4+Q5+Q6}{6}$ $= 50\%$
	Q2	$\frac{0}{0} = 100\%$	
	Q3	$\frac{0}{5} = 0\%$	
	Q4	$\frac{0}{5} = 0\%$	
	Q5	$\frac{6}{6} = 100\%$	
	Q6	$\frac{0}{8} = 0\%$	
Availability	Q1	$\sum_{n=1}^{5} \frac{\frac{(node(n)\ connections)}{4}}{5} = 60\%$	$\frac{Q1+Q2}{2}$

	Q2	$\frac{\sum_{n=1}^{1}\frac{3}{5}}{\#1} = 60\%$	$= 60\%$

Table 41: Measurement n3c7

Authentication	Q1	$\frac{5}{5} = 100\%$	$\frac{Q1+Q2+Q3}{3}$ $= 100\%$
	Q2	$\frac{5}{5} = 100\%$	
	Q3	$\frac{1}{1} = 100\%$	
Authorization	Q1	$\frac{5}{5} = 100\%$	$\frac{Q1+Q2}{2}$ $= 100\%$
	Q2	$\frac{5}{5} = 100\%$	
Transaction confidentiality	Q1	$\frac{6}{6} = 100\%$	$\frac{Q1+Q2}{2}$ $= 70\%$
	Q2	$\frac{2}{5} = 40\%$	
Transaction integrity	Q1	$\frac{6}{6} = 100\%$	$\frac{Q1+Q2}{2}$ $= 70\%$
	Q2	$\frac{2}{5} = 40\%$	
Perimeter security	Q1	$\frac{0}{0} = 100\%$	$\frac{Q1+Q2+Q3+Q4+Q5+Q6}{6}$ $= 50\%$
	Q2	$\frac{0}{0} = 100\%$	
	Q3	$\frac{0}{5} = 0\%$	
	Q4	$\frac{0}{5} = 0\%$	
	Q5	$\frac{6}{6} = 100\%$	
	Q6	$\frac{0}{8} = 0\%$	
Availability	Q1	$\frac{\sum_{n=1}^{5}\frac{(node(n)\ connections)}{4}}{5} =$ 60%	$\frac{Q1+Q2}{2}$
	Q2	$\frac{\sum_{n=1}^{1}\frac{3}{5}}{\#1} = 60\%$	$= 60\%$

Table 42: Measurement n3c8

Authentication	Q1	$\frac{5}{5} = 100\%$	$\frac{Q1+Q2+Q3}{3}$ $= 100\%$
	Q2	$\frac{5}{5} = 100\%$	
	Q3	$\frac{1}{1} = 100\%$	
Authorization	Q1	$\frac{5}{5} = 100\%$	$\frac{Q1+Q2}{2}$ $= 100\%$
	Q2	$\frac{5}{5} = 100\%$	
Transaction confidentiality	Q1	$\frac{5}{6} = 83,33\%$	$\frac{Q1+Q2}{2}$ $= 91,66\%$
	Q2	$\frac{5}{5} = 100\%$	
Transaction integrity	Q1	$\frac{5}{6} = 83,33\%$	$\frac{Q1+Q2}{2}$ $= 91,66\%$
	Q2	$\frac{5}{5} = 100\%$	
Perimeter security	Q1	$\frac{0}{0} = 100\%$	$\frac{Q1+Q2+Q3+Q4+Q5+Q6}{6}$ $= 50\%$
	Q2	$\frac{0}{0} = 100\%$	
	Q3	$\frac{0}{5} = 0\%$	
	Q4	$\frac{0}{5} = 0\%$	
	Q5	$\frac{6}{6} = 100\%$	
	Q6	$\frac{0}{8} = 0\%$	
Availability	Q1	$\frac{\sum_{n=1}^{5}\frac{(node(n)\ connections)}{4}}{5} =$ 60%	$\frac{Q1+Q2}{2}$
	Q2	$\frac{\sum_{n=1}^{1}\frac{3}{5}}{\#1} = 60\%$	$= 60\%$

Authentication	Q1	$\frac{5}{5} = 100\%$	$\frac{Q1+Q2+Q3}{3}$ $= 100\%$
	Q2	$\frac{5}{5} = 100\%$	
	Q3	$\frac{1}{1} = 100\%$	
Authorization	Q1	$\frac{5}{5} = 100\%$	$\frac{Q1+Q2}{2}$ $= 100\%$
	Q2	$\frac{5}{5} = 100\%$	
Transaction confidentiality	Q1	$\frac{8}{8} = 100\%$	$\frac{Q1+Q2}{2}$ $= 50\%$
	Q2	$\frac{0}{5} = 0\%$	
Transaction integrity	Q1	$\frac{8}{8} = 100\%$	$\frac{Q1+Q2}{2}$ $= 50\%$
	Q2	$\frac{0}{5} = 0\%$	
Perimeter security	Q1	$\frac{0}{0} = 100\%$	$\frac{Q1+Q2+Q3+Q4+Q5+Q6}{6}$ $= 50\%$
	Q2	$\frac{0}{0} = 100\%$	
	Q3	$\frac{0}{5} = 0\%$	
	Q4	$\frac{0}{5} = 0\%$	
	Q5	$\frac{8}{8} = 100\%$	
	Q6	$\frac{0}{8} = 0\%$	
Availability	Q1	$\frac{\sum_{n=1}^{5} \frac{(node(n)\ connections)}{4}}{5} = 80\%$	$\frac{Q1+Q2}{2}$ $= 70\%$
	Q2	$\frac{\sum_{n=1}^{1} \frac{3}{5}}{\#1} = 60\%$	

Table 25: Measurement n2c7

Table 43: Measurement n3c9

Authentication	Q1	$\frac{5}{5} = 100\%$	$\frac{Q1+Q2+Q3}{3}$ $= 100\%$
	Q2	$\frac{5}{5} = 100\%$	
	Q3	$\frac{1}{1} = 100\%$	
Authorization	Q1	$\frac{5}{5} = 100\%$	$\frac{Q1+Q2}{2}$ $= 100\%$
	Q2	$\frac{5}{5} = 100\%$	
Transaction confidentiality	Q1	$\frac{4}{6} = 66,66\%$	$\frac{Q1+Q2}{2}$ $= 83,33\%$
	Q2	$\frac{5}{5} = 100\%$	
Transaction integrity	Q1	$\frac{4}{6} = 66,66\%$	$\frac{Q1+Q2}{2}$ $= 83,33\%$
	Q2	$\frac{5}{5} = 100\%$	
Perimeter security	Q1	$\frac{0}{0} = 100\%$	$\frac{Q1+Q2+Q3+Q4+Q5+Q6}{6}$ $= 50\%$
	Q2	$\frac{0}{0} = 100\%$	
	Q3	$\frac{0}{5} = 0\%$	
	Q4	$\frac{0}{5} = 0\%$	
	Q5	$\frac{6}{6} = 100\%$	
	Q6	$\frac{0}{8} = 0\%$	
Availability	Q1	$\frac{\sum_{n=1}^{5} \frac{(node(n)\ connections)}{4}}{5} = 60\%$	$\frac{Q1+Q2}{2}$ $= 60\%$
	Q2	$\frac{\sum_{n=1}^{1} \frac{3}{5}}{\#1} = 60\%$	

Table 44: Measurement n1c10

Authentication	Q1	$\frac{5}{5} = 100\%$	$\frac{Q1+Q2+Q3}{3}$ $= 100\%$
	Q2	$\frac{5}{5} = 100\%$	
	Q3	$\frac{1}{1} = 100\%$	
Authorization	Q1	$\frac{5}{5} = 100\%$	$\frac{Q1+Q2}{2}$ $= 100\%$
	Q2	$\frac{5}{5} = 100\%$	
Transaction confidentiality	Q1	$\frac{4}{6} = 66,66\%$	$\frac{Q1+Q2}{2}$ $= 73,33\%$
	Q2	$\frac{4}{5} = 100\%$	
Transaction integrity	Q1	$\frac{4}{6} = 66,66\%$	$\frac{Q1+Q2}{2}$ $= 83,33\%$
	Q2	$\frac{5}{5} = 100\%$	
Perimeter security	Q1	$\frac{0}{0} = 100\%$	$\frac{Q1+Q2+Q3+Q4+Q5+Q6}{6}$ $= 50\%$
	Q2	$\frac{0}{0} = 100\%$	
	Q3	$\frac{0}{5} = 0\%$	
	Q4	$\frac{0}{} = 0\%$	

	Q2	$\frac{5}{5} = 100\%$	$= 100\%$
	Q3	$\frac{1}{1} = 100\%$	
Authorization	Q1	$\frac{5}{5} = 100\%$	$\frac{Q1+Q2}{2}$
	Q2	$\frac{5}{5} = 100\%$	$= 100\%$
Transaction confidentiality	Q1	$\frac{4}{6} = 66,66\%$	$\frac{Q1+Q2}{2}$
	Q2	$\frac{3}{5} = 60\%$	$= 63,33\%$
Transaction integrity	Q1	$\frac{4}{6} = 66,66\%$	$\frac{Q1+Q2}{2}$
	Q2	$\frac{5}{5} = 100\%$	$= 83,33\%$
Perimeter security	Q1	$\frac{0}{0} = 100\%$	$\frac{Q1+Q2+Q3+Q4+Q5+Q6}{6}$
	Q2	$\frac{0}{0} = 100\%$	$= 50\%$
	Q3	$\frac{0}{5} = 0\%$	
	Q4	$\frac{0}{5} = 0\%$	
	Q5	$\frac{6}{6} = 100\%$	
	Q6	$\frac{0}{8} = 0\%$	
Availability	Q1	$\frac{\sum_{n=1}^{5} \frac{(node(n)\ connections)}{4}}{5} = 60\%$	$\frac{Q1+Q2}{2}$
	Q2	$\frac{\sum_{n=1}^{1} \frac{3}{5}}{\#1} = 60\%$	$= 60\%$

Table 46: Measurement n3c12

Authentication	Q1	$\frac{5}{5} = 100\%$	$\frac{Q1+Q2+Q3}{3}$
	Q2	$\frac{5}{5} = 100\%$	$= 100\%$
	Q3	$\frac{1}{1} = 100\%$	
Authorization	Q1	$\frac{5}{5} = 100\%$	$\frac{Q1+Q2}{2}$
	Q2	$\frac{5}{5} = 100\%$	$= 100\%$
Transaction confidentiality	Q1	$\frac{4}{6} = 66,66\%$	$\frac{Q1+Q2}{2}$
	Q2	$\frac{2}{5} = 40\%$	$= 53,33\%$
Transaction integrity	Q1	$\frac{4}{6} = 66,66\%$	$\frac{Q1+Q2}{2}$
	Q2	$\frac{5}{5} = 100\%$	$= 83,33\%$
Perimeter security	Q1	$\frac{0}{0} = 100\%$	$\frac{Q1+Q2+Q3+Q4+Q5+Q6}{6}$
	Q2	$\frac{0}{0} = 100\%$	$= 50\%$
	Q3	$\frac{0}{5} = 0\%$	
	Q4	$\frac{0}{5} = 0\%$	
	Q5	$\frac{6}{6} = 100\%$	
	Q6	$\frac{0}{8} = 0\%$	
Availability	Q1	$\frac{\sum_{n=1}^{5} \frac{(node(n)\ connections)}{4}}{5} = 60\%$	$\frac{Q1+Q2}{2}$
	Q2	$\frac{\sum_{n=1}^{1} \frac{3}{5}}{\#1} = 60\%$	$= 60\%$

Table 47: Measurement n3c13

Authentication	Q1	$\frac{5}{5} = 100\%$	$\frac{Q1+Q2+Q3}{3}$
	Q2	$\frac{5}{5} = 100\%$	$= 100\%$
	Q3	$\frac{1}{1} = 100\%$	
Authorization	Q1	$\frac{5}{5} = 100\%$	$\frac{Q1+Q2}{2}$

	Q2	$\frac{5}{5} = 100\%$	$= 100\%$
Transaction confidentiality	Q1	$\frac{4}{6} = 66,66\%$	$\frac{Q1+Q2}{2}$
	Q2	$\frac{2}{5} = 40\%$	$= 53,33\%$
Transaction integrity	Q1	$\frac{4}{6} = 66,66\%$	$\frac{Q1+Q2}{2}$
	Q2	$\frac{4}{5} = 80\%$	$= 73,33\%$
Perimeter security	Q1	$\frac{0}{0} = 100\%$	$\frac{Q1+Q2+Q3+Q4+Q5+Q6}{6}$
	Q2	$\frac{0}{0} = 100\%$	$= 50\%$
	Q3	$\frac{0}{5} = 0\%$	
	Q4	$\frac{0}{5} = 0\%$	
	Q5	$\frac{6}{6} = 100\%$	
	Q6	$\frac{0}{8} = 0\%$	
Availability	Q1	$\frac{\sum_{n=1}^{5} \frac{(node(n)\ connections)}{4}}{5} = 60\%$	$\frac{Q1+Q2}{2}$
	Q2	$\frac{\sum_{n=1}^{1} \frac{3}{5}}{\#1} = 60\%$	$= 60\%$

Table 48: Measurement n3c14

Authentication	Q1	$\frac{5}{5} = 100\%$	$\frac{Q1+Q2+Q3}{3}$
	Q2	$\frac{5}{5} = 100\%$	$= 100\%$
	Q3	$\frac{1}{1} = 100\%$	
Authorization	Q1	$\frac{5}{5} = 100\%$	$\frac{Q1+Q2}{2}$
	Q2	$\frac{5}{5} = 100\%$	$= 100\%$
Transaction confidentiality	Q1	$\frac{4}{6} = 66,66\%$	$\frac{Q1+Q2}{2}$
	Q2	$\frac{2}{5} = 40\%$	$= 53,33\%$
Transaction integrity	Q1	$\frac{4}{6} = 66,66\%$	$\frac{Q1+Q2}{2}$
	Q2	$\frac{3}{5} = 60\%$	$= 63,33\%$
Perimeter security	Q1	$\frac{0}{0} = 100\%$	$\frac{Q1+Q2+Q3+Q4+Q5+Q6}{6}$
	Q2	$\frac{0}{0} = 100\%$	$= 50\%$
	Q3	$\frac{0}{5} = 0\%$	
	Q4	$\frac{0}{5} = 0\%$	
	Q5	$\frac{6}{6} = 100\%$	
	Q6	$\frac{0}{8} = 0\%$	
Availability	Q1	$\frac{\sum_{n=1}^{5} \frac{(node(n)\ connections)}{4}}{5} = 60\%$	$\frac{Q1+Q2}{2}$
	Q2	$\frac{\sum_{n=1}^{1} \frac{3}{5}}{\#1} = 60\%$	$= 60\%$

Table 49: Measurement n3c15

Authentication	Q1	$\frac{5}{5} = 100\%$	$\frac{Q1+Q2+Q3}{3}$
	Q2	$\frac{5}{5} = 100\%$	$= 100\%$
	Q3	$\frac{1}{1} = 100\%$	
Authorization	Q1	$\frac{5}{5} = 100\%$	$\frac{Q1+Q2}{2}$
	Q2	$\frac{5}{5} = 100\%$	$= 100\%$
Transaction confidentiality	Q1	$\frac{4}{6} = 66,66\%$	$\frac{Q1+Q2}{2}$
	Q2	$\frac{2}{5} = 40\%$	$= 53,33\%$

Transaction integrity	Q1	$\frac{4}{6} = 66,66\%$	$\frac{Q1+Q2}{2}$
	Q2	$\frac{2}{5} = 40\%$	$= 53,33\%$
Perimeter security	Q1	$\frac{0}{0} = 100\%$	$\frac{Q1+Q2+Q3+Q4+Q5+Q6}{6}$
	Q2	$\frac{0}{0} = 100\%$	$= 50\%$
	Q3	$\frac{0}{5} = 0\%$	
	Q4	$\frac{0}{5} = 0\%$	
	Q5	$\frac{6}{6} = 100\%$	
	Q6	$\frac{0}{8} = 0\%$	
Availability	Q1	$\frac{\sum_{n=1}^{5} \frac{(node(n)\ connections)}{4}}{5} = 60\%$	$\frac{Q1+Q2}{2}$
	Q2	$\frac{\sum_{n=1}^{1} \frac{3}{5}}{\#1} = 60\%$	$= 60\%$

A.4 Network 4

Table 50: Measurement n4c1

Authentication	Q1	$\frac{5}{5} = 100\%$	$\frac{Q1+Q2+Q3}{3}$
	Q2	$\frac{5}{5} = 100\%$	$= 100\%$
	Q3	$\frac{1}{1} = 100\%$	
Authorization	Q1	$\frac{5}{5} = 100\%$	$\frac{Q1+Q2}{2}$
	Q2	$\frac{5}{5} = 100\%$	$= 100\%$
Transaction confidentiality	Q1	$\frac{5}{5} = 100\%$	$\frac{Q1+Q2}{2}$
	Q2	$\frac{5}{5} = 100\%$	$= 100\%$
Transaction integrity	Q1	$\frac{5}{5} = 100\%$	$\frac{Q1+Q2}{2}$
	Q2	$\frac{5}{5} = 100\%$	$= 100\%$
Perimeter security	Q1	$\frac{0}{0} = 100\%$	$\frac{Q1+Q2+Q3+Q4+Q5+Q6}{6}$
	Q2	$\frac{0}{0} = 100\%$	$= 50\%$
	Q3	$\frac{0}{5} = 0\%$	
	Q4	$\frac{0}{5} = 0\%$	
	Q5	$\frac{6}{6} = 100\%$	
	Q6	$\frac{0}{8} = 0\%$	
Availability	Q1	$\frac{\sum_{n=1}^{5} \frac{(node(n)\ connections)}{4}}{5} = 50\%$	$\frac{Q1+Q2}{2}$
	Q2	$\frac{\sum_{n=1}^{1} \frac{3}{5}}{\#1} = 60\%$	$= 60\%$

Table 51: Measurement n4c2

Authentication	Q1	$\frac{5}{5} = 100\%$	$\frac{Q1+Q2+Q3}{3}$
	Q2	$\frac{5}{5} = 100\%$	$= 100\%$
	Q3	$\frac{1}{1} = 100\%$	
Authorization	Q1	$\frac{5}{5} = 100\%$	$\frac{Q1+Q2}{2}$
	Q2	$\frac{5}{5} = 100\%$	$= 100\%$
Transaction confidentiality	Q1	$\frac{5}{5} = 100\%$	$\frac{Q1+Q2}{2}$
	Q2	$\frac{3}{5} = 60\%$	$= 80\%$
Transaction	Q1	$\frac{5}{5} = 100\%$	$\frac{Q1+Q2}{2}$

integrity	Q2	$\frac{5}{5} = 100\%$	$= 100\%$
Perimeter security	Q1	$\frac{0}{0} = 100\%$	$\frac{Q1+Q2+Q3+Q4+Q5+Q6}{6}$ $= 50\%$
	Q2	$\frac{0}{0} = 100\%$	
	Q3	$\frac{0}{5} = 0\%$	
	Q4	$\frac{0}{5} = 0\%$	
	Q5	$\frac{6}{6} = 100\%$	
	Q6	$\frac{0}{8} = 0\%$	
Availability	Q1	$\frac{\sum_{n=1}^{5} \frac{(node(n)\ connections)}{4}}{5} =$ 50%	$\frac{Q1+Q2}{2}$
	Q2	$\frac{\sum_{n=1}^{1} \frac{3}{5}}{\#1} = 60\%$	$= 60\%$

A.4.1 Configuration 3

We keep configuration 2. Support for receiving, sending and forwarding messages with confidentiality protection is removed from the node lc3.

Table 52: Measurement n4c3

Authentication	Q1	$\frac{5}{5} = 100\%$	$\frac{Q1+Q2+Q3}{3}$ $= 100\%$
	Q2	$\frac{5}{5} = 100\%$	
	Q3	$\frac{1}{1} = 100\%$	
Authorization	Q1	$\frac{5}{5} = 100\%$	$\frac{Q1+Q2}{2}$ $= 100\%$
	Q2	$\frac{5}{5} = 100\%$	
Transaction confidentiality	Q1	$\frac{5}{5} = 100\%$	$\frac{Q1+Q2}{2}$ $= 80\%$
	Q2	$\frac{3}{5} = 60\%$	
Transaction integrity	Q1	$\frac{5}{5} = 100\%$	$\frac{Q1+Q2}{2}$ $= 100\%$
	Q2	$\frac{5}{5} = 100\%$	
Perimeter security	Q1	$\frac{0}{0} = 100\%$	$\frac{Q1+Q2+Q3+Q4+Q5+Q6}{6}$ $= 50\%$
	Q2	$\frac{0}{0} = 100\%$	
	Q3	$\frac{0}{5} = 0\%$	
	Q4	$\frac{0}{5} = 0\%$	
	Q5	$\frac{6}{6} = 100\%$	
	Q6	$\frac{0}{8} = 0\%$	
Availability	Q1	$\frac{\sum_{n=1}^{5} \frac{(node(n)\ connections)}{4}}{5} =$ 50%	$\frac{Q1+Q2}{2}$
	Q2	$\frac{\sum_{n=1}^{1} \frac{3}{5}}{\#1} = 60\%$	$= 60\%$

A.4.2 Configuration 3

We keep configuration 2. Support for receiving, sending and forwarding messages with confidentiality protection is removed from the node lc3.

Table 53: Measurement n4c3

Authentication	Q1	$\frac{5}{5} = 100\%$	$\frac{Q1+Q2+Q3}{3}$ $= 100\%$
	Q2	$\frac{5}{5} = 100\%$	

	Q3	$\frac{1}{1} = 100\%$	
Authorization	Q1	$\frac{5}{5} = 100\%$	$\frac{Q1+Q2}{2}$
	Q2	$\frac{5}{5} = 100\%$	$= 100\%$
Transaction confidentiality	Q1	$\frac{5}{5} = 100\%$	$\frac{Q1+Q2}{2}$
	Q2	$\frac{3}{5} = 60\%$	$= 80\%$
Transaction integrity	Q1	$\frac{5}{5} = 100\%$	$\frac{Q1+Q2}{2}$
	Q2	$\frac{5}{5} = 100\%$	$= 100\%$
Perimeter security	Q1	$\frac{0}{0} = 100\%$	$\frac{Q1+Q2+Q3+Q4+Q5+Q6}{6}$
	Q2	$\frac{0}{0} = 100\%$	$= 50\%$
	Q3	$\frac{0}{5} = 0\%$	
	Q4	$\frac{0}{5} = 0\%$	
	Q5	$\frac{6}{6} = 100\%$	
	Q6	$\frac{0}{8} = 0\%$	
Availability	Q1	$\sum_{n=1}^{5} \frac{\frac{(node(n)\ connections)}{4}}{5} = 50\%$	$\frac{Q1+Q2}{2}$
	Q2	$\frac{\sum_{n=1}^{1} \frac{3}{5}}{\#1} = 60\%$	$= 60\%$

Table 54: Measurement n4c4

Authentication	Q1	$\frac{5}{5} = 100\%$	$\frac{Q1+Q2+Q3}{3}$
	Q2	$\frac{5}{5} = 100\%$	$= 100\%$
	Q3	$\frac{1}{1} = 100\%$	
Authorization	Q1	$\frac{5}{5} = 100\%$	$\frac{Q1+Q2}{2}$
	Q2	$\frac{5}{5} = 100\%$	$= 100\%$
Transaction confidentiality	Q1	$\frac{5}{5} = 100\%$	$\frac{Q1+Q2}{2}$
	Q2	$\frac{3}{5} = 60\%$	$= 80\%$
Transaction integrity	Q1	$\frac{5}{5} = 100\%$	$\frac{Q1+Q2}{2}$
	Q2	$\frac{4}{5} = 80\%$	$= 90\%$
Perimeter security	Q1	$\frac{0}{0} = 100\%$	$\frac{Q1+Q2+Q3+Q4+Q5+Q6}{6}$
	Q2	$\frac{0}{0} = 100\%$	$= 50\%$
	Q3	$\frac{0}{5} = 0\%$	
	Q4	$\frac{0}{5} = 0\%$	
	Q5	$\frac{6}{6} = 100\%$	
	Q6	$\frac{0}{8} = 0\%$	
Availability	Q1	$\sum_{n=1}^{5} \frac{\frac{(node(n)\ connections)}{4}}{5} = 50\%$	$\frac{Q1+Q2}{2}$
	Q2	$\frac{\sum_{n=1}^{1} \frac{3}{5}}{\#1} = 60\%$	$= 60\%$

Table 55: Measurement n4c5

Authentication	Q1	$\frac{5}{5} = 100\%$	$\frac{Q1+Q2+Q3}{3}$
	Q2	$\frac{5}{5} = 100\%$	$= 100\%$
	Q3	$\frac{1}{1} = 100\%$	
Authorization	Q1	$\frac{5}{5} = 100\%$	$\frac{Q1+Q2}{2}$
	Q2	$\frac{5}{5} = 100\%$	$= 100\%$

Transaction confidentiality	Q1	$\frac{5}{5} = 100\%$	$\frac{Q1+Q2}{2}$ $= 80\%$
	Q2	$\frac{3}{5} = 60\%$	
Transaction integrity	Q1	$\frac{5}{5} = 100\%$	$\frac{Q1+Q2}{2}$ $= 80\%$
	Q2	$\frac{3}{5} = 60\%$	
Perimeter security	Q1	$\frac{0}{0} = 100\%$	$\frac{Q1+Q2+Q3+Q4+Q5+Q6}{6}$ $= 50\%$
	Q2	$\frac{0}{0} = 100\%$	
	Q3	$\frac{0}{5} = 0\%$	
	Q4	$\frac{0}{5} = 0\%$	
	Q5	$\frac{6}{6} = 100\%$	
	Q6	$\frac{0}{8} = 0\%$	
Availability	Q1	$\frac{\sum_{n=1}^{5} \frac{(node(n)\ connections)}{4}}{5} = 50\%$	$\frac{Q1+Q2}{2}$
	Q2	$\frac{\sum_{n=1}^{1} \frac{3}{5}}{\#1} = 60\%$	$= 60\%$

Table 56: Measurement n4c6

Authentication	Q1	$\frac{5}{5} = 100\%$	$\frac{Q1+Q2+Q3}{3}$ $= 100\%$
	Q2	$\frac{5}{5} = 100\%$	
	Q3	$\frac{1}{1} = 100\%$	
Authorization	Q1	$\frac{5}{5} = 100\%$	$\frac{Q1+Q2}{2}$ $= 100\%$
	Q2	$\frac{5}{5} = 100\%$	
Transaction confidentiality	Q1	$\frac{4}{5} = 80\%$	$\frac{Q1+Q2}{2}$ $= 90\%$
	Q2	$\frac{5}{5} = 100\%$	
Transaction integrity	Q1	$\frac{4}{5} = 80\%$	$\frac{Q1+Q2}{2}$ $= 90\%$
	Q2	$\frac{5}{5} = 100\%$	
Perimeter security	Q1	$\frac{0}{0} = 100\%$	$\frac{Q1+Q2+Q3+Q4+Q5+Q6}{6}$ $= 50\%$
	Q2	$\frac{0}{0} = 100\%$	
	Q3	$\frac{0}{5} = 0\%$	
	Q4	$\frac{0}{5} = 0\%$	
	Q5	$\frac{6}{6} = 100\%$	
	Q6	$\frac{0}{8} = 0\%$	
Availability	Q1	$\frac{\sum_{n=1}^{5} \frac{(node(n)\ connections)}{4}}{5} = 50\%$	$\frac{Q1+Q2}{2}$
	Q2	$\frac{\sum_{n=1}^{1} \frac{3}{5}}{\#1} = 60\%$	$= 60\%$

Table 57: Measurement n4c7

Authentication	Q1	$\frac{5}{5} = 100\%$	$\frac{Q1+Q2+Q3}{3}$ $= 100\%$
	Q2	$\frac{5}{5} = 100\%$	
	Q3	$\frac{1}{1} = 100\%$	
Authorization	Q1	$\frac{5}{5} = 100\%$	$\frac{Q1+Q2}{2}$ $= 100\%$
	Q2	$\frac{5}{5} = 100\%$	
Transaction confidentiality	Q1	$\frac{4}{5} = 80\%$	$\frac{Q1+Q2}{2}$ $= 80\%$
	Q2	$\frac{4}{5} = 80\%$	

Transaction integrity	Q1	$\frac{4}{5} = 80\%$	$\frac{Q1+Q2}{2} = 90\%$
	Q2	$\frac{5}{5} = 100\%$	
Perimeter security	Q1	$\frac{0}{0} = 100\%$	$\frac{Q1+Q2+Q3+Q4+Q5+Q6}{6} = 50\%$
	Q2	$\frac{0}{0} = 100\%$	
	Q3	$\frac{0}{5} = 0\%$	
	Q4	$\frac{0}{5} = 0\%$	
	Q5	$\frac{6}{6} = 100\%$	
	Q6	$\frac{0}{8} = 0\%$	
Availability	Q1	$\frac{\sum_{n=1}^{5} \frac{(node(n)\ connections)}{4}}{5} = 50\%$	$\frac{Q1+Q2}{2} = 60\%$
	Q2	$\frac{\sum_{n=1}^{1} \frac{3}{5}}{\#1} = 60\%$	

Table 58: Measurement n4c8

Authentication	Q1	$\frac{5}{5} = 100\%$	$\frac{Q1+Q2+Q3}{3} = 100\%$
	Q2	$\frac{5}{5} = 100\%$	
	Q3	$\frac{1}{1} = 100\%$	
Authorization	Q1	$\frac{5}{5} = 100\%$	$\frac{Q1+Q2}{2} = 100\%$
	Q2	$\frac{5}{5} = 100\%$	
Transaction confidentiality	Q1	$\frac{4}{5} = 80\%$	$\frac{Q1+Q2}{2} = 70\%$
	Q2	$\frac{3}{5} = 60\%$	
Transaction integrity	Q1	$\frac{4}{5} = 80\%$	$\frac{Q1+Q2}{2} = 90\%$
	Q2	$\frac{5}{5} = 100\%$	
Perimeter security	Q1	$\frac{0}{0} = 100\%$	$\frac{Q1+Q2+Q3+Q4+Q5+Q6}{6} = 50\%$
	Q2	$\frac{0}{0} = 100\%$	
	Q3	$\frac{0}{5} = 0\%$	
	Q4	$\frac{0}{5} = 0\%$	
	Q5	$\frac{6}{6} = 100\%$	
	Q6	$\frac{0}{8} = 0\%$	
Availability	Q1	$\frac{\sum_{n=1}^{5} \frac{(node(n)\ connections)}{4}}{5} = 50\%$	$\frac{Q1+Q2}{2} = 60\%$
	Q2	$\frac{\sum_{n=1}^{1} \frac{3}{5}}{\#1} = 60\%$	

Table 59: Measurement n4c9

Authentication	Q1	$\frac{5}{5} = 100\%$	$\frac{Q1+Q2+Q3}{3} = 100\%$
	Q2	$\frac{5}{5} = 100\%$	
	Q3	$\frac{1}{1} = 100\%$	
Authorization	Q1	$\frac{5}{5} = 100\%$	$\frac{Q1+Q2}{2} = 100\%$
	Q2	$\frac{5}{5} = 100\%$	
Transaction confidentiality	Q1	$\frac{4}{5} = 80\%$	$\frac{Q1+Q2}{2} = 70\%$
	Q2	$\frac{3}{5} = 60\%$	
Transaction integrity	Q1	$\frac{4}{5} = 80\%$	$\frac{Q1+Q2}{2} = 80\%$
	Q2	$\frac{4}{5} = 80\%$	

Perimeter security	Q1	$\frac{0}{0} = 100\%$	$\frac{Q1+Q2+Q3+Q4+Q5+Q6}{6}$ $= 50\%$
	Q2	$\frac{0}{0} = 100\%$	
	Q3	$\frac{0}{5} = 0\%$	
	Q4	$\frac{0}{5} = 0\%$	
	Q5	$\frac{6}{6} = 100\%$	
	Q6	$\frac{0}{8} = 0\%$	
Availability	Q1	$\frac{\sum_{n=1}^{5}\frac{(node(n)\ connections)}{4}}{5} = 50\%$	$\frac{Q1+Q2}{2}$ $= 60\%$
	Q2	$\frac{\sum_{n=1}^{1}\frac{3}{5}}{\#1} = 60\%$	

Table 60: Measurement n4c10

Authentication	Q1	$\frac{5}{5} = 100\%$	$\frac{Q1+Q2+Q3}{3}$ $= 100\%$
	Q2	$\frac{5}{5} = 100\%$	
	Q3	$\frac{1}{1} = 100\%$	
Authorization	Q1	$\frac{5}{5} = 100\%$	$\frac{Q1+Q2}{2}$ $= 100\%$
	Q2	$\frac{5}{5} = 100\%$	
Transaction confidentiality	Q1	$\frac{4}{5} = 80\%$	$\frac{Q1+Q2}{2}$ $= 70\%$
	Q2	$\frac{3}{5} = 60\%$	
Transaction integrity	Q1	$\frac{4}{5} = 80\%$	$\frac{Q1+Q2}{2}$ $= 80\%$
	Q2	$\frac{4}{5} = 80\%$	
Perimeter security	Q1	$\frac{0}{0} = 100\%$	$\frac{Q1+Q2+Q3+Q4+Q5+Q6}{6}$ $= 50\%$
	Q2	$\frac{0}{0} = 100\%$	
	Q3	$\frac{0}{5} = 0\%$	
	Q4	$\frac{0}{5} = 0\%$	
	Q5	$\frac{6}{6} = 100\%$	
	Q6	$\frac{0}{8} = 0\%$	
Availability	Q1	$\frac{\sum_{n=1}^{5}\frac{(node(n)\ connections)}{4}}{5} = 50\%$	$\frac{Q1+Q2}{2}$ $= 60\%$
	Q2	$\frac{\sum_{n=1}^{1}\frac{3}{5}}{\#1} = 60\%$	