2012

Flow analysis based on role and pattern matching

Pooja Wagh

Rochester Institute of Technology

B. Thomas Golisano College

Of

Computing and Information Sciences

Master of Science in

Computing Security and Information Assurance

Thesis Approval Form

Student Name: Pooja Suresh Wagh

Thesis Title: Flow Analysis Based on role and Pattern Matching

Thesis Committee

Name	Signature	Date

Prof. Charles Border
Primary Advisor – R.I.T. Dept. of Networking, Security, and Systems Administration

---

Prof. Peter Lutz
Secondary Advisor – R.I.T. Dept. of Networking, Security, and Systems Administration

---

Prof. Luther Troell
Secondary Advisor – R.I.T. Dept. of Networking, Security, and Systems Administration

Thesis Release Permission Form

Rochester Institute of Technology

B. Thomas Golisano College of Computing and Information Sciences

Title: Flow Analysis based on Role and Pattern Matching

I, Pooja Wagh, hereby grant permission to the Wallace Memorial Library to reproduce my thesis in whole or part.

_____

Pooja S. Wagh

_____

Date

Dedication

This paper is dedicated to my parents. Without their support and guidance, the report wouldn't have been completed. I would also like to dedicate this paper to all my friends who continually supported me throughout the writing process.

Acknowledgements

I would like to thank my committee advisor, Charles Border, and my committee members, Peter Lutz and Luther Troell, for their assistance and guidance throughout the thesis process.

Abstract

Flow analysis has always been a great concern for network security. An attacker can gain important information through several ways by monitoring the frequency and timing of network packets or by impersonating another user through remote access. To evaluate the flow of packets through the network and extract the unknown packets is a challenging task for a network administrator.

An access to any network asset depends on the flow arriving from the source. Most of the organizations have built their networks to regulate the traffic flow based on the authenticity of the source. However, allowing access based on simple authentication (username and password) is nothing but monitoring the perimeter around the network leaving a company's network wide open for the inside threat.

Based on the above model, there is a necessity to develop network architecture to reduce or eliminate threats within the organization. This research present a new network model built around the idea of analyzing data flows to determine whether it is possible for an untrusted flow to "earn" its way into becoming a trusted flow based on notion of user's activity matching a specified pattern affiliated with the role.

Table of contents

List of Figures

List of Tables

Chapter 1 Introduction

As the use of the Internet grows, so does the number of threats associated with it. These threats are becoming a great concern for network security. Every day new hacking tools and scripts are being used to compromise networks across the globe. It is the responsibility of the network administrator to analyze the nature and source of information abuse and any such incidents occurring in the network. Any data flowing into the network is suspect, as the source of the data flow may not be completely known to the network. Much research has been done to provide a clear understanding of how a network system can be safeguarded against malicious attacks.

A basic approach and most popular to network security involves analyzing the source of the data flowing into the network and preventing unauthorized access based on the source of the network flow. Most security mechanisms differentiate between two kinds of flow: a flow from a trusted source and one from an untrusted source. Determining if a flow is from a trusted flow is not always an easy task, since it might be camouflaged to appear as though it originated from a trusted source to gain easy access to the network. Also, promoting network security solely on the basis of a dichotomy of ‘trusted’ or ‘untrusted’ sources could involve questioning as no definite check exits to prove the legitimacy of the flow.

The network model proposed in this study involves a type of packet filtering known as Deep Packet Inspection that assays each packet of a flow as it passes through an inspection point (router)to test for any irregularities compared to the implemented policy and determine if the flow is to be placed in the whitelist category. If the flow is judge to be from a whitelisted source, it is directed towards the production server. However, if the router cannot match the data flow to

a pre-defined whitelisted source, the router will redirect the flow to the covert environment network, where the activities will be logged and compared to a profile of expected activities affiliated with the role. If after a period of analysis the profile of activities is matched, the flow will be released from the covert network and routed towards the production server.

Consider the following scenarios:

Scenario1: Trusted Flow

A new flow getting connected to the network will be examined for the IP address. If the router finds a match with a pre-existing whitelist, the flow is considered trusted and will be directed to the production server.

Scenario2: Unknown/Untrusted Flow (matching pattern activity)

If the IP address is not on the pre-existing whitelist, the flow is routed to the covert network where the flow activities will be monitored and matched against a pattern of expected activities defined for the role associated with the user name used to authenticate to the network. If after a period of interactions the length of which can be determined based on the security status of the role, the flow matches the activity pattern associated with a role, the system will release the flow from the covert network and direct it to the production network and update the whitelist with the IP address of the flow.

Scenario3: Unknown/Untrusted Flow (does not match the activity pattern)

If after a period of interactions, the expected activity pattern is not matched by the activities of flow, the flow will be considered malicious and the packet inspector will contact the router to

terminate the flow's connection with the network. Also, all activities related to the flow will be rolled back based on logs.

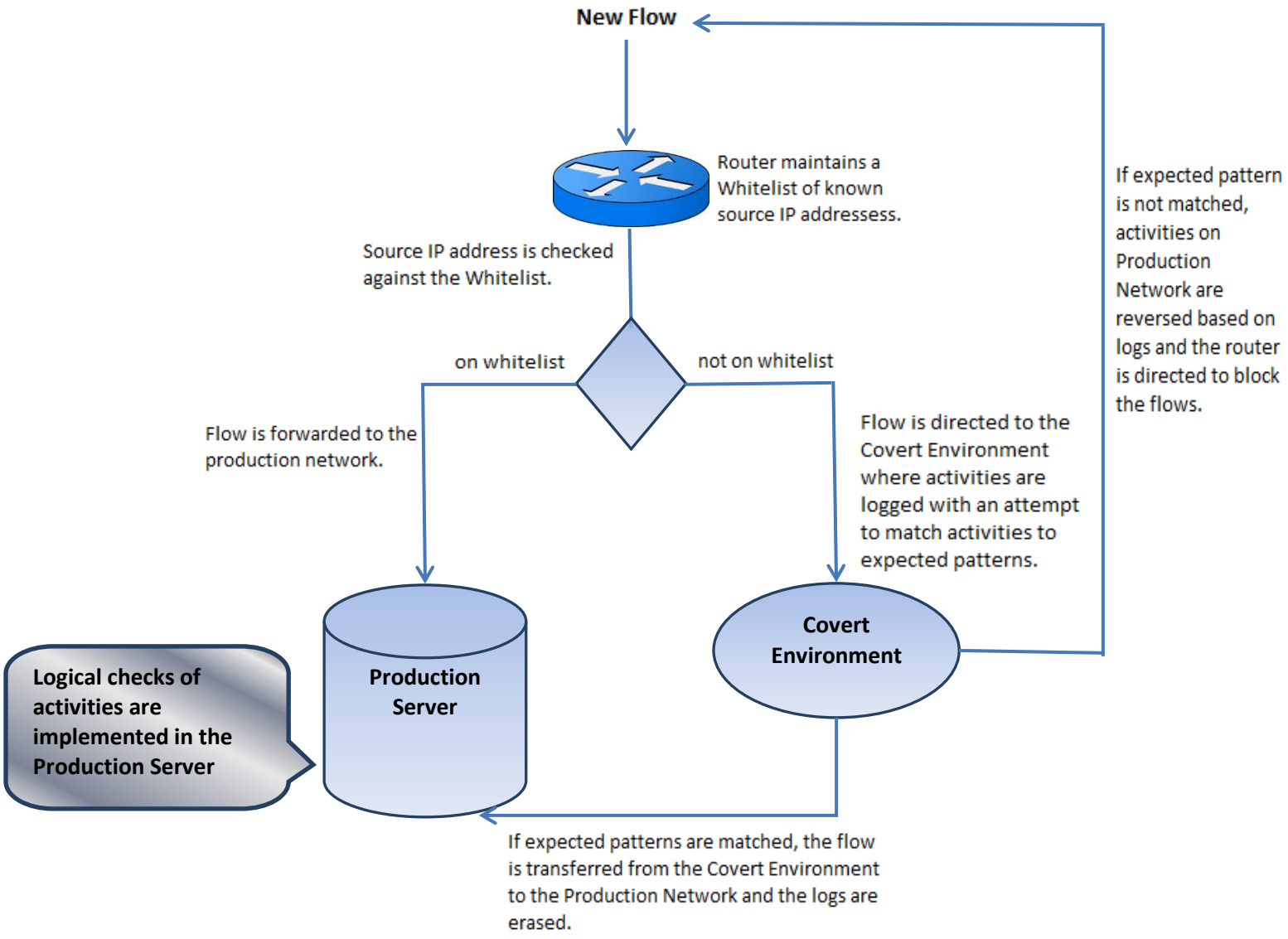


Figure1: Structure of a new flow entering the network

Normally, due to the amount of traffic on a production network, it is difficult to log the level of detail that security practitioners need to make accurate judgments. A covert network is similar to a Honeynet, in that it involves involving a network of actual systems running real operating

systems and services. In this research the covert network is very similar to the traditional Honeynet except that it is envisioned to have a greatly increased logging facility that can be used to roll back activities of flows that do not match expected patterns and are therefore judged as malicious. The covert network therefore gives the administrator the ability to learn more about the attacks and attackers than they might have experienced in traditional network architecture along with the ability to roll back potentially malicious activities based on the enhanced logging facility. However, these networks do not have any production value and hence any activity occurring in the covert environment is deemed to be from an attacker where the activities can be logged and analyzed in a much more intensive fashion.

This thesis uses the covert network as a platform to log untrusted activities and attempt to match those activities to the pattern of expected activities. This network would be responsible for monitoring the activities of untrusted connections and routing those flow connections that match the pre-defined role based activities to the production network. Further, the covert network will contact the router to update the whitelist with flow information based on username-password combination.

RBAC roles

Roles are the mechanism used to assign authorizations to a flow based on their competencies and responsibilities in the organization. A network administrator provides a set of predefined roles for system management. These roles are stored in the local role database of a network. This set of roles is intended to group typical administrative responsibilities.

When a flow is assigned a role, the flow is given no more privilege than is necessary to accomplish the role. Use of roles to control access can be an effective mean for developing and

enforcing enterprise-specific security policies, and for streamlining the security management process. *[“Configuring Role-Based Access Control” October 2010].*

Sub-role: A user having authorization for a different role.

Assigning a role to a flow allows the flow to access the role and use the authorizations that are contained in the role. A network administrator provides direct assignment of authorizations to a role or the indirect assignment of authorizations through a sub-role. A sub-role can be specified for a role in the role list attribute of a role. Configuring a role to have a designated sub-role effectively assigns all of the authorizations in the sub-role to the role. Hence if a flow has an authorization to perform activity related to a different role, the flow can still continue performing that activity and be part of the role implemented by the network’s policy.

A system administrator can assign a role to multiple flows and can assign multiple roles to a flow. A flow which has been assigned multiple roles can activate more than one role simultaneously if necessary to perform system management functions.

Example: A flow has been defined for multiple roles; a 'Superadmin', an 'Admin', and a 'Volunteer'. They have access to different (sometimes overlapping) role functions. To give Admin a Volunteer role, simply make Volunteer a child of Admin. If Admin is made a child of Superadmin, then the user who is a Superadmin will also be an Admin. So logically Volunteer becomes a child of Superadmin and Superadmin gets the role of Volunteer.

Role Migration.

In certain scenarios where, a role defined for a flow is to be changed to new role, the network administrator will redefine the existing role to a current role using several role-management

commands available to list, create, modify, and remove roles. Roles can be created with the '**mkrole'** command, modified with the '**chrole'** command, removed with the '**rmrole'** command, and displayed with the '**lsrole'** command.

Following are the requirements while creating a new role or changing an existing role to a new role:

- Assigning appropriate name to a role depending on the flow's efficiency and skills to act on the role.
- Providing an insight to the flow's capabilities before re-defining or assigning a role.
- Deciding upon the authorizations required for the role.
- Considering whether authorizations should be directly assigned to the role or indirectly assigned to the role through a sub-role.
- Assigning the flow with different credentials for accessing the new role.
- Authenticating the flow while activating the role.

When a flow authenticates to the system, the flow's session does not have any associated roles or authorizations. In order to associate roles to the session, the flow must invoke a separate authentication command (the **swrole** command) to switch to the role or roles.

Hence whenever a flow logs into his account to perform any activity, apart from its credentials, the flow is expected to authorize itself to the network based on the newly assigned role.

Also when new versions of roles are being assigned to flows, migration of these roles will be updated in a file for the new functionality while maintaining the current role abilities.

In the proposed architecture, a certain profile of activity is attached to a role. If the flow's actual activity matches the expected role profile activity, the flow will be released from the covert network and routed directly to the production server. While the flow is active in the covert environment, its activity will be logged and then transferred to the production environment. The flow will be unaware of it being routed to the covert network and any mismatch of activities in the production environment will lead to termination of the flow's connection with the network.

Large organizations will find this network model a benefit in their ability to know a flow's activity and will allow access to sensitive information only to those flows that do not pose any threat to network system.

My thesis aspires to hold all untrusted flows in the covert network to scrutinize their activities and help them earn their way out to the production server based on roles assigned to the flows in conjunction with matching a pre-defined set of activities that the flow must oblige to.

1.1 Problem Summary

With the evolution of the Internet, system security has become a matter of concern. People are getting more and more dependent on the Internet that involves from sending emails to a friend to conducting online banking transactions. As the use of the Internet makes our lives more effortless, at the same time with the expansion of internet applications, various methods of exploiting internet security also increases. It is the responsibility of the system administrator to be aware of the methods that a hacker might use to exploit the network. In today's large scale and globally interconnected networks, identifying legitimate flows from the malicious one is extremely difficult.

Allowing network access solely on the basis of single factor authentication, will armor against any malicious flow entering into the system, but will fail to detect any unauthorized flow camouflaging as an authorized one.

This thesis proposes a model that would initially route all untrusted flows in a covert network where all the flow activities will be monitored in an attempt to match an actual pattern of activities against an expected pattern of activities based on a role. In order to earn their way to the production server, all flows within the covert environment must follow a pre-defined set of activities and must abide to the role assigned to them.

1.2 Importance

With the advent of numerous network technologies, the risk of untrusted sources gaining network access and exploiting it has increased. This thesis aims in analyzing the unknown flows and judging them based on pattern matching and roles assigned to them.

With the number of users accessing an Internet application, it is likely that many unknown flows will gain access to the network without fully being authorized. Hence, it is essential that we segregate the new flow connection based on the IP addresses in the whitelist maintained by the router.

This framework has been built for examining the new flow arrivals into the network and monitoring the activities of untrusted flows within the covert environment by matching the role and activities that the flows are required to follow.

1.3 Purpose Statement

Accomplishing a network access based on a single factor authentication is insufficient to judge the flow's legitimacy. This thesis will classify the flows in two categories: a trusted flow and untrusted flow. The purpose of this research is to monitor the activities of untrusted flows within the covert network to help the flows earn their way to the production server.
The flow categorized as untrusted is sub-divided into those flows that match the pattern activity based on their assigned role and earn their way to become trusted flows. Those flows that fail to match the expected pattern of activity will eventually be disconnected from the network.

This research aims at presenting a written document based on a suitable model for implementing network security in any enterprise to determine certified flows for access. The notion would be to design a network model that will route all untrusted flows into the covert environment and direct only those flows to the production server whose IP addresses match a whitelist. In addition, the thesis points to the use of pattern activity that the flows must follow in order to earn their way out of the covert network. The secondary important aspect is the use of 'covert network' as a tool to provide detailed logging to track flow activity in the network until an adequate amount of traffic has been received to determine if the activity matches that expected for the flow based on the assigned role.

1.4 Document Outline

The paper is outlined as follows:

The first section covers the basic definitions such as Flow analysis, Intrusion Detection system[IDS]/ Intrusion Prevention System [IPS], the notion of Role Based Access Control

(RBAC), relationship between users and role, use of covert network, pattern activity and usage of role in home environment.

Following this, the document discusses the key concepts used for this model: authentication and authorization and the control access that play a major role in determining the flow's legitimacy. Further the document briefly talks about the traditional systems for detecting intrusion and how can these intruding flows earn their way to become trusted flows and gain resources from the production server. Summary and conclusion are presented with a discussion on future research objective.

1.5 Introduction to Flow Analysis

Flow analysis is the industry-standard method of collecting and recording network flows. Flow analysis allows seeing what type of flows pass through the network, without having to reproduce the problem. With this definition in mind, we examine whether the new flow entering the network is trusted or untrusted based on a set of whitelisted IP addresses that the router holds. The IP addresses of the flows matching the whitelist are directly routed to the production server and those not on the whitelist will be examined in the covert network based on pattern matching and role concept.

1.6 Literature Review

The idea for this model is derived from several papers based on a role and matching activity pattern.

1.6.1 Role Analysis Pattern

Roles are what any concept (or class) would play within the context of its related concepts (or classes). For instance a “company” would be the “supplier” of some specific “product”, where “Supplier” being a role. Software and Business modeling analyst Fransis G.Mosse discusses the ways if solving the Role problems through one of the 5 role patterns: Role Inheritance, Association Roles, Role Classes, Generalized Role Classes and Association Class Roles. Though the role problems are not described explicitly, the author explains every role problem solution in detail.

Each role pattern has a specific characteristic approach towards a role problem. This research has brought to light the use of pattern activity for observing the movements of untrusted flows within the covert environment. This feature is blended with the role concept to follow a pre-defined set of activities and match the patterns corresponding to the role assigned. *[Mosse, F. G., n.d.]*

1.6.2 Relationship between Users and Roles

A bulletin on’ An Introduction to Role-Based Access Control’ by NIST/ITL provides a background information on RBAC as a means of controlling access to network resources. Research on access control technology has been conducted that addressed monitoring unauthorized admits to classified information depending on roles and operations associated with roles *[NIST/ITL Bulletin, 1995]*.

Under the RBAC framework, every user is associated with a role. For instance, a School Institution decides that the role of a student must be constrained only to view the grades of their courses without undergoing any changes that would lead to the violation of institutional rules.

This thesis monitors every activity of the flow within the covert network for any infringement or mismatch of activity pattern based on role assigned to the flow.

Authors have been able to proof the competency of RBAC in large organization based on experiments carried out by the Object Management Group (OMG) and Common Object Request Broker Architecture (CORBA).

1.6.3 Honeynet mechanism

Honeynets have been designed as a network of actual systems running real operating systems and services. The article 'Pakistan Honeynet Project' has introduced the concept of Honeynet as a technology used to gather information about motives and tactics of the Black-Hat community targeting Pakistan networks.

Honeynet is an architecture composed of multiple technologies and products. The architecture depends on the way it is deployed. Author Faiz Ahmad emphasizes on deployment of Honeynet using the following 3 mechanisms:

1.6.3.1 Data Control

Data control is a tool for tracking the activity to and from the Honeynet. There are three techniques for implementing data control i.e. connection control, bandwidth control and intrusion prevention, that make a powerful data controlling system. Connection control is used to limit the outbound connections from the Honeynet, whereas Bandwidth control manages both inbound and outbound network bandwidth for the Honeynet. Intrusion prevention blocks the known attacks by inspecting every packet at the gateway matching them with the IDS rules.

1.6.3.2 Data Capture

Data capture helps to log as much information without attackers knowing it. Sebek is one of the tools used for logging attacker's activity on the Honeynet, which is installed as a hidden kernel module.

A recommended feature is to store the captured data on a secured remote system rather than storing locally. It reduces the chances of attackers detecting the captured data, and deleting or modifying it.

1.6.3.3 Data Collection

The purpose of data collection is to centrally capture and combine the information collected from multiple Honeynet deployments.

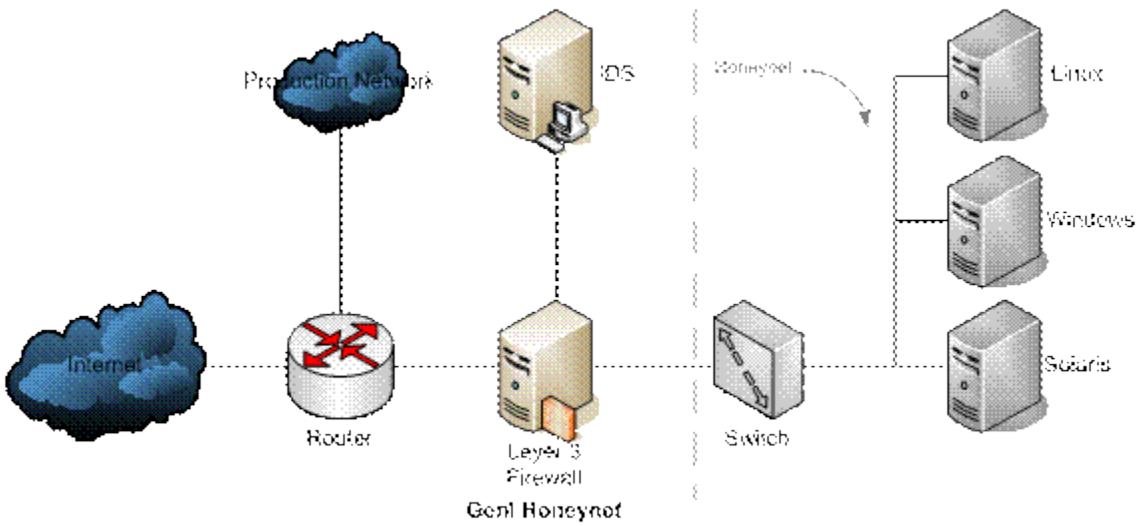


Figure2.1 GENI Architecture[1].

[1]Based on fig. from "Pakistan Honeynet Project".

GENI architecture was developed implementing these three mechanisms. The GENI Honeynet was developed to capture the maximum amount of attacker activity and give them a feel of real network. However there were some downsides in this architecture that did not comply with features necessary for capturing advanced attacks. Identifying the issues and problems in GENI I, GENI II, was developed that include IPS in alternative to IDS, having enhanced logging system and ability to block or modify the attacks.

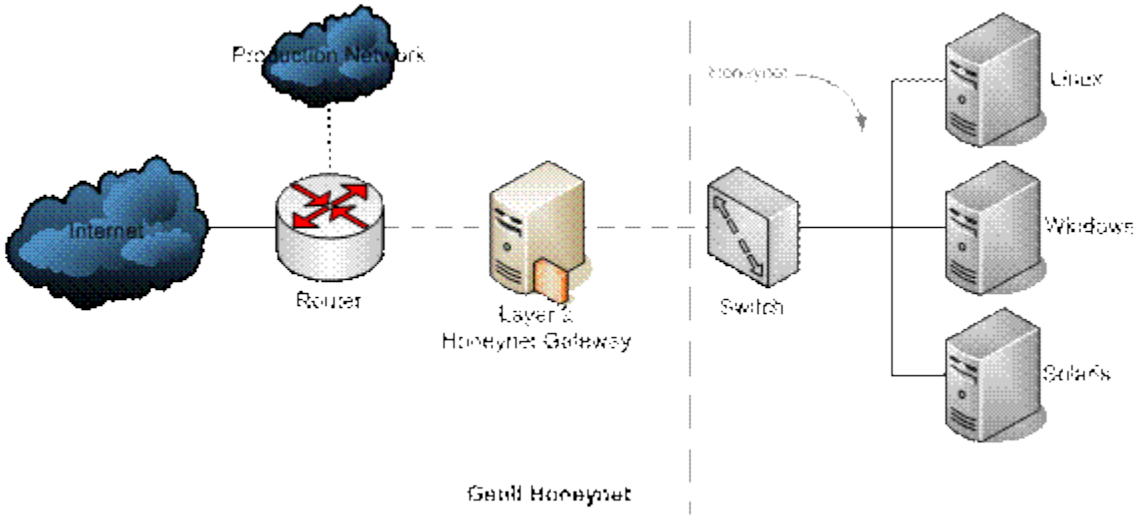


Figure 2.2GENI II Architecture[2].

The study was beneficial in applying the concept of 'Honeynet' to the covert Environment that kept a log of flow activities and secretly monitored in an attempt to match the flow activity with a pre-existing set of activity pattern based on a role.

The study was also beneficial in understanding the psychology of the attack and implement techniques for future use. *[Shuja, 2004]*.

[2] Based on fig. from "Pakistan Honeynet Project".

1.6.4 Configuring RBAC framework

One of the most challenging problems in managing large network is the complexity of security administration. The article 'Cisco Application Control Engine Module Getting Started Guide' provides a basic understanding of how ACE (Application Control Engine) provides security administration based on RBAC while configuring the permissions to access the resources of a network.

The authors have addressed a series of predefined roles assigned to users followed by a tabular structure describing RBAC configuration.

Table1: RBAC Configuration[3].

Procedure

	Command	Purpose
Step 1	**changeto** *context* **Example:** host1/Admin# changeto VC_WEB host1/VC_WEB#	Changes to the correct context if necessary. Check the CLI prompt to verify that you are operating in the VC_WEB context.
Step 2	**config** **Example:** host1/VC_WEB# config host1/VC_WEB(config)#	Enters configuration mode.
Step 3	**domain** *name* **Example:** host1/VC_WEB(config)# domain DOMAIN1 host1/VC_WEB(config-domain)#	Creates a domain for the context.
Step 4	**add-object all** **Example:** host1/VC_WEB(config-domain)# add-object all	Allocates all configuration objects in the VC_WEB context to the domain.
Step 5	**exit** **Example:** host1/VC_WEB(config-domain)# exit host1/VC_WEB(config)#	Exits domain configuration mode.

[3]Based on "Cisco Application Control Engine Module-Getting Started Guide".

Table1 (*contd*.)

	Command	Purpose
Step 6	**username** *user* **password 5** *password* **role** *name1* **domain** *name2* **Example:** host1/VC_WEB(config)# username USER1 password 5 1vAN9gQDI$MmbmjQgJPj45lxbtzXPpB1 role Server-Maintenance domain DOMAIN1 host1/VC_WEB(config)# exit	Configures new user USER1, and assigns the predefined role SLB-Admin and the domain DOMAIN1 to USER1 The **5** parameter for the **password** keyword requires that you enter an MD5 hash-encrypted password. You can obtain an MD5 hash password by first entering the **username** command with the **0** parameter and a clear-text password (for example, MYPASSWORD). Next, enter the **show running-config** command and copy the user's encrypted password from the running-configuration file. Enter the username command again using the **5** parameter and the encrypted password.
Step 7	**exit** **Example:** host1/VC_WEB(config)# exit host1/VC_WEB#	Exits configuration mode.
Step 8	**show running-config role** **show running config domain** **Examples:** host1/VC_WEB# show running-config role host1/VC_WEB# show running-config domain	Displays the user and domain configurations.
Step 9	**copy running-config startup-config** **Example:** host1/VC_WEB# copy running-config startup-config	(Optional) Copies the running configuration to the startup configuration.

This thesis uses a RBAC framework to allow roles to be assigned to the flows and monitor their activity within the network to check for a match for a flow activity against a set of expected activities based on the role assigned. *[Configuring Role-Based Access Control, 2010]*.

1.6.5 User Activity Pattern

A report on 'Patterns of User Activity in the Blackboard Course management at Brigham Young University'(Griffiths) discusses the use of Blackboard course management in terms of use of pattern activity as records in the database that contains a set of data represented by set of

tables and graph that summarize activity performed by students, professors and assistants. The activities are summarized on basis of different categories of users and a specific pattern that the users follow while performing the operations on the dataset.

Course management study (CMS) has a greater impact in large institutions to study usage patterns and making the necessary recommendations of usage levels that will serve any questions related to sizing and scoping hardware and network requirements. The author has greatly emphasized on this study as it is observed a beneficial perception for both students and faculty of Blackboard University.

The Blackboard database is stored in an Oracle database on a server that is housed at a Blackboard site of BYU campus. The author has put forth a step-by-step action of collecting and sorting the Blackboard data describing a series of clicks carried by the Blackboard community. This campus-wide data was analyzed to find general patterns of activity with a set of questions related to study.

[Michael] shows concerns for some part of the study that weren't fully absorbed during the analysis.

A report was generated as a series of questionnaire followed by the data that constitutes the results of this study stated in numerical figures, tables, and charts. The report depicts a wide variety of Blackboard activity and explores these usage patterns for a database.
[Michael] provides a useful framework in implementing the pattern activity, illustrating the series of activities specific to a flow and effectively monitoring the flows for a pattern that the flow must follow in order to earn it way towards the production server. *[Griffiths, 2007]*.

1.6.6 IDS/IPS

The paper" Understanding IPS and IDS: Using IPS and IDS together for Defense in Depth" by SANS Institute, focuses on the most recent use of networks by placing the values of both technologies, Intrusion Detection System(IDS) and Intrusion Prevention System (IPS) and deploying them together to provide a stronger security posture.

At its basic, IDS is a passive device, watching the packets flowing through the network, comparing the traffic to configured rules, and setting off an alarm if it detects anything suspicious. An intrusion prevention system is used to actively drop packets of data or disconnect connections that contain unauthorized data. Intrusion prevention technology is also commonly an extension of intrusion detection technology. Further the paper takes up a next step in identifying the security parameters once the technology was discovered and their vulnerabilities were noted.

One way to determine these security parameters is to build a formula to represent the idea of security.

Security = visibility + control

[Holland] have suggested an architecture that employs both IPS and IDS technologies used together to positively influence an organizational security posture.

[Holland] have rolled into the details of deploying the two technologies showing concerns for high performance as the IDs implementation have the tendency to drop packets that might cause loss of information, leading to data unavailability factor, due to the high throughput of high bandwidth network devices. Another concern being encryption, that have the inability to

decrypt packets making the security administrators unaware about what is coming into and going out of corporate networks.

[Holland] has come up with the challenge in finding qualified and skilled security staff for deploying either IPS or IDS that requires specialized skills. Using both technologies in harmony, the authors will provide the needed perimeter to defend the existing threat and also having the visibility into internal networks with the ability to provide forensic data and trend analysis *[Holland, 2004]*.

1.6.7 Usage of Role in Home Network Environment

To offer secure home services, home network environments provide access control over various home devices and information when users want to access. Authors, Do-Woo, Geon-Woo, Lee and Han presented a paper 'Role-Based Access Control Model in Home Network Environment' proposing a access control model using RBAC in home environments to provide home users with secure home services.

Access Control is defined as means by which the ability is explicitly enabled or restricted in some way. Using role based access control, access decisions are based on the roles that individual users have as part of an organization.

This thesis applies the concept of role, as it helps the network administrator know the flow activity based on the role each flow plays in order to prove itself trusted and earn a way out to achieve the access to the production system.

With RBAC, security is managed at a level that corresponds closely to the organization's structure. Each user is assigned with a role and every role has been assigned with one or more

than one privileges. RBAC grants rights and permissions to roles rather than individual users. Users then acquire the rights and permissions by being assigned to appropriate roles.

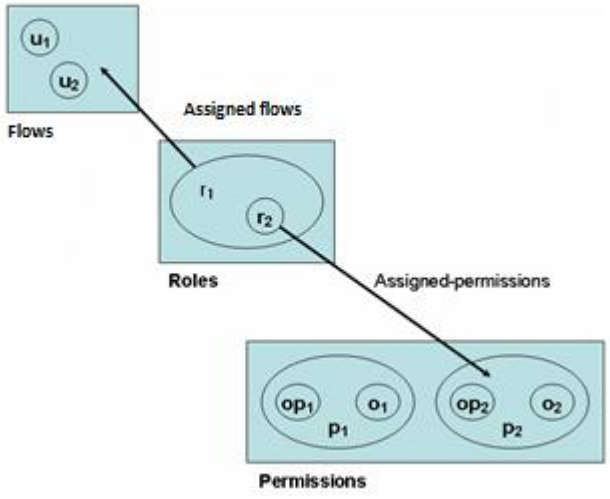
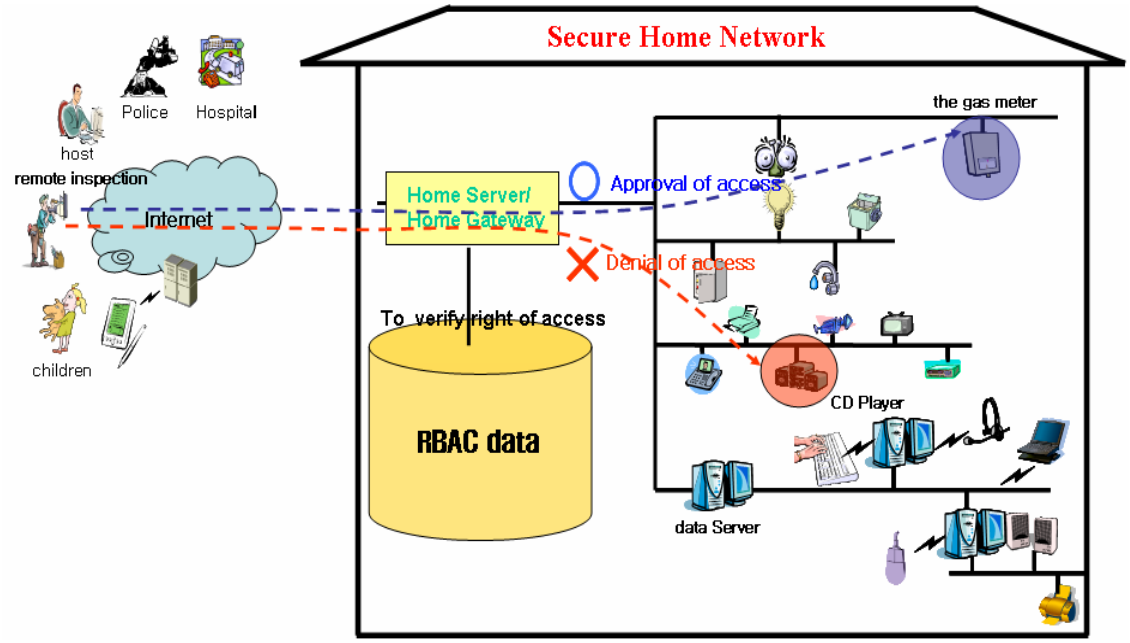


Figure 3: User, role, permission relationships[4]

[Kim, D.-W., Kim, G. W., Lee, J.-H., & Han, J.-W] describes the application of RBAC model while providing an example of one-to-one and one-to-many relationship of a role and user, i.e., the network administrator assigning a meter role to A, having permission to access gas meter and to B, the access to gas meter as well a CD player. In such scenario, user A can access the gas meter but not the CD player whereas user B has access to both services.

[4]Based on fig. from "Modeling Roles: A practical series of Analysis Patterns"



The example proved successful in implementing RBAC in home networks and offered enhanced secure home services by presenting the access control model in home network environments *[Kim, D.-W., Kim, G. W., Lee, J.-H., & Han, J.-W., 2005]*.

[5]Based on fig. from "Role-based Access Control Model in Home Network Environments"

Chapter 2 Methodology

The development of this model was based on research of existing literature related to the area of study, in addition to discussion with industry and academic experts. The concept of flow analysis has been developed as a great concern for network security.

Analyzing flow within the network would require developing a model that will allow untrusted flows earn their way to become trusted ones in an attempt to match the pattern activity based on their assigned role. The model involves a router that holds the whitelisted IP addresses and analyses the incoming flows based on those known IP addresses. If the router founds a match for an IP address in the whitelist, the flow will be directed to the production server; else the flow will be routed to the covert environment for further surveillance. The flows in the covert network will be monitored based on whether the untrusted flows fulfill the pre-defined set of activities assigned with their role. If the flow's activities match the expected set of activities, the flow would be released from the covert network and routed to the production server. If the flow fails to match the pattern, its activities will be rolled back and all the related logs will be erased.

The covert network maintains an encrypted log file that records flow details and is responsible to keep check on the pattern of activities assigned to each flow based on the role.

2.1Scenarios

Scenario 1: *When the flow abides to a role and matches the pattern activity assigned to it.*

Suppose, if a source is identified as web developer, he is responsible for monitoring the development side of the organization, i.e., develop a website, configure HTML, XML output properties, work on embedded style sheets, etc. If the flow sticks to this pattern, eventually the

system will consider the flow as a trusted flow and will release it from the covert network for the flow to earn its way towards the production server.

Scenario 2: *When the flow approaches to any activity not associated with its role:*

Suppose a flow is assigned a Student role where its activity pattern involves logging into the account, viewing academic profile and hitting the Grades button to view the grades. If the flow goes against its profile of activities and clicks the Edit Grades option, the system will sense a breach in the network and will immediately contact the administrator to look in for the logs containing the details of the flow. The administrator will check for the role assigned and the pattern of activity the flow must have assumed. The administrator considers this as an intrusion to the system, thereby preventing the flow for any further access to the network resources. All the related logs to that flow will be erased from the log directory and the flow activities will be reversed.

The covert network is responsible to communicate with the router to update the routing table notifying the changes made to the flow.

Once the system senses no more breaches in the network, the administrator will scan the covert network for any malicious activity and update the production server.

Finally when all the up gradations are done, the network administrator will route the authorized flow to the production server and equip the resources.

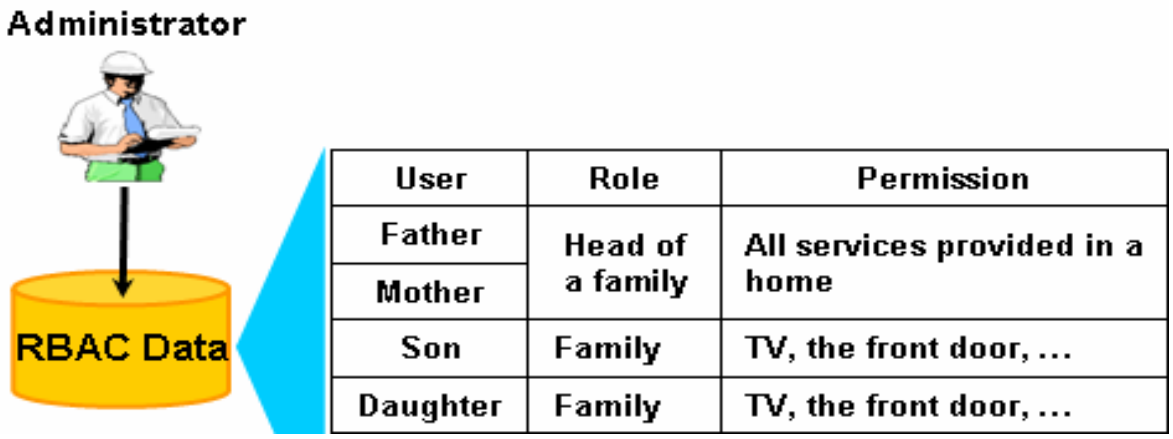
Chapter 3 Results and Analyses

3.1 Key Concepts

3.1.1 Access control

Access control is the means by which the ability is explicitly enabled or restricted in some way (usually through physical and system-based controls).

As stated by authors (Do-Woo Kim, Geon Woo Kim, Jun-Ho Lee, and Jong-Wook Han) in RBAC model in Home Network Environments [7], access control is often required to offer secure home services in a home network environment for various home devices.
In RBAC framework, access decisions are based on an individual's roles and responsibilities within the organization or user base. With RBAC, A home network system administrator can create roles according to the job functions performed in a home. For example, a system administrator can assign a father and mother to the head of a family and a son and daughter as a teenager role.



User	Role	Permission
Father	Head of a family	All services provided in a home
Mother		
Son	Family	TV, the front door, …
Daughter	Family	TV, the front door, …

Figure 5: Definition of roles and permissions for RBAC[6]

[6]Based on fig. from "Role-based Access Control Model in Home Network Environments"

Access control technology has evolved from research and development efforts supported by the Department of Defense (DoD). With role-based access control, access decisions are based on the roles that individual users have as part of an organization. Users take on assigned roles (such as doctor, nurse, teller, manager). The process of defining roles comes from the access control technology and is based on a thorough analysis of how an organization should operate in controlling the rights of the users based on roles.

3.1.2 Relationship between flow and packets

Although flow based solutions are great, there are some areas where packet capture is still needed. Flow data in most cases does not provide TCP timing and application response times. We cannot see the issues involved in file transfer, i.e., which files are being called in an application, what response codes are involved at an application level, service response time such as DNS and DHCP, as well as several other statistics that are critical in application performance troubleshooting.

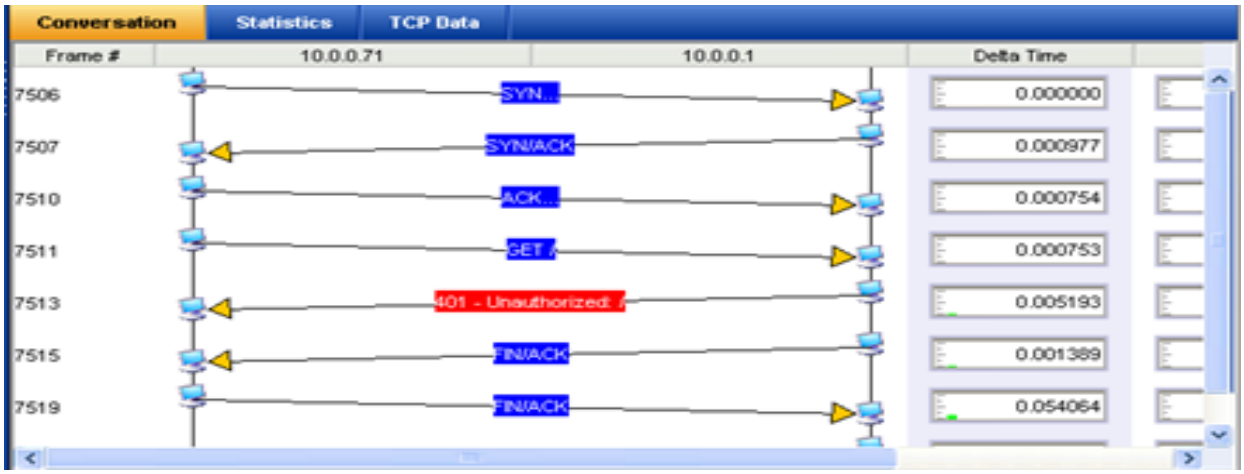


Figure 6: Analysis of client conversation with statistical view of traffic within the network along with the TCP timing and application response times[7].

For this reason, when analyzing an application, packet capture solutions are critical to have in place as it views the actual packets involved in client conversations and get to the root cause of the issue. Flows can help to determine traffic statistics overall, but it falls short when we need to analyze a specific conversation in depth.

My thesis entails the concept of flow analysis for monitoring flows in the network and alarming any aberrant activity in the network, while the covert network will be responsible for monitoring and reporting any performance issues (acting against the ascribed Role or pattern activity).

[7]Based on fig. from blog "Packet Capture vs. Flow Collection: Which one do I need in a monitoring solution?"

3.1.3Value of Data Flow

The value of data flow depends on several factors, including regulatory, productivity and the known/unknown values of flows. These factors analyze the new arrivals to determine whether the flows should be directed to the production server or into the covert network.

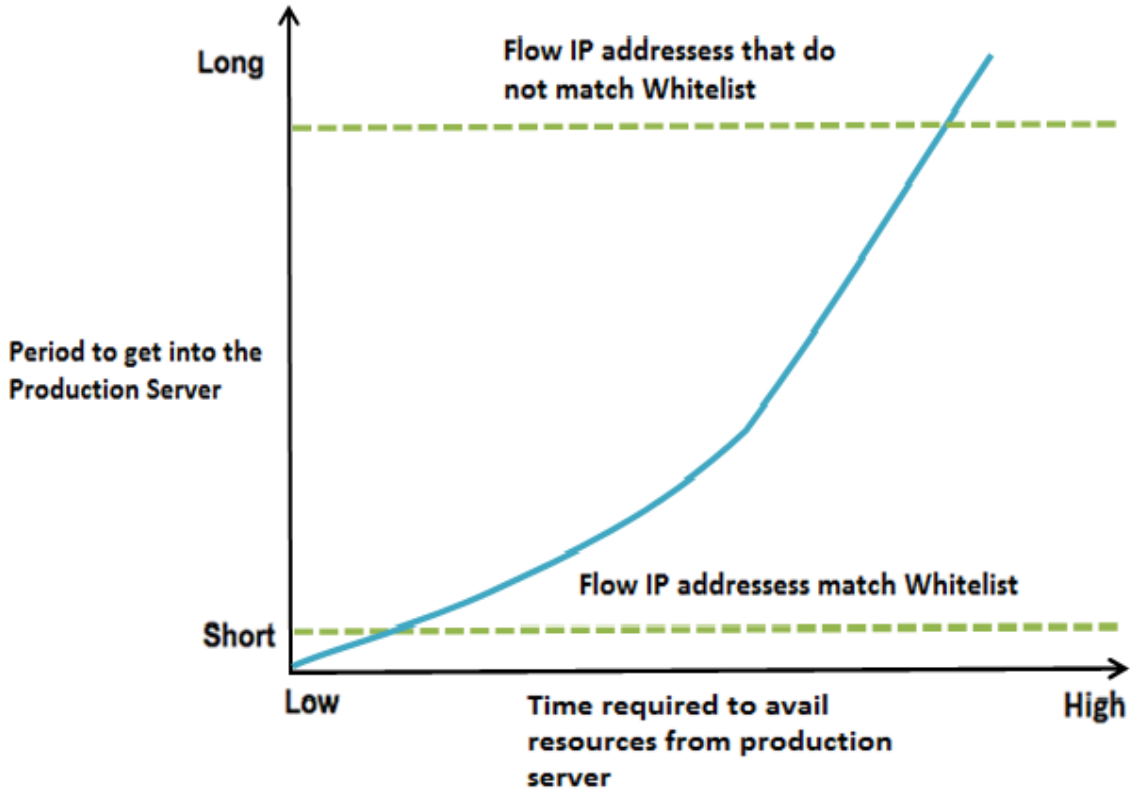


Figure 7: Analyses the new flow arriving into the network

The above factors also affect the length of time a flow stays in the covert environment, as shown in the graph below:

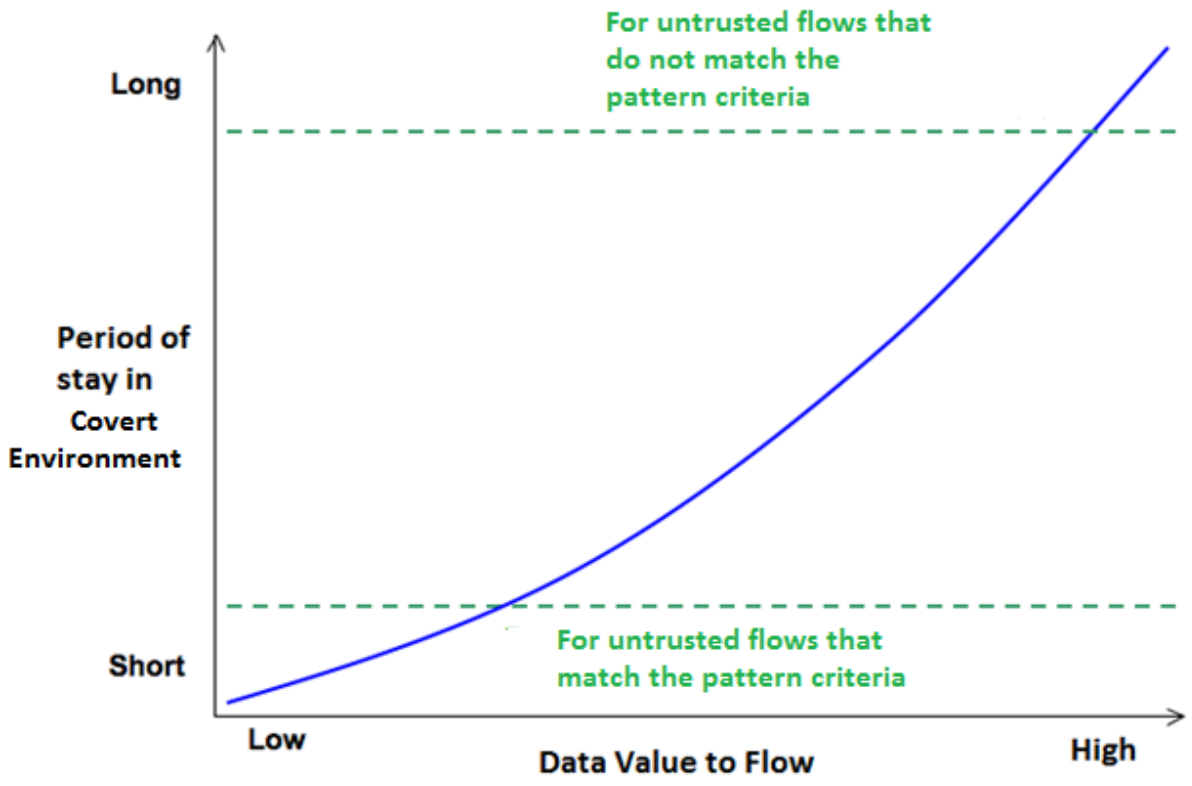


Figure 8: Depicts the amount of time period a flow to be monitored for its activities in the covert network.

3.1.3.1 Regulatory

Flows arriving from the source are usually authenticated before they access the network resources. The flows are monitored for their activities to validate their legitimacy. The Sarbanes-Oxley act (SOX) states that applicable business records must be retained in full for a period of no

less than five years [SOX]. Those flows that do not match the known IP addresses in the whitelist, those flows are directed towards the covert network for regulatory purpose and the time constraints depends on the flow being licit to be admissible into the production server.

3.1.3.2 Productivity

Stored flow value is often treasured for its correlation to productivity, and the need to have certain information for the purpose of conducting analysis of the activities carried out by these flows. An encrypted log file in the covert environment accounts for logging all the detailed information on flows and attempts to match the activities with the expected set of activities based on Pattern Matching approach *[Hardware Pattern Matching for Network Traffic Analysis in Gigabit]*.

With this in mind, productivity data fits well into the scope of the flow analysis framework, as a master copy of the records of flow activities would be inscribed in the encrypted file directory for the administrator to look in whenever any aberrant activity takes place in the server.

3.1.3.3 Value of Known flow

Depending on the source IP address, the value of the flow can be known considering the fact that the flow is arriving from a known IP address.

Example: For provincial reign organizations, i.e. ‘Cisco Network Solutions’, featuring Cisco Routers & Switches Flexible Financing provider, the IP address/ Mac address can be recognizable based on single factor authentication. However the source will be completely authorized to the network once it follows the protocols of the company’s network designed to fulfill the security constraints. Such flows may only be needed to stay in the covert network for short-term and could be re-directed to the production server after further analysis.

3.1.3.4 Value of Unknown Flow

This category includes those sources outside the provincial domain whose IP address is imperceptible to the network and needs intense surveillance over the flows.

Example: For the world's largest Russian gas company 'Gazprom', would be required to be regulated and retained for a long-term in the system for security purposes. Sarbanes-Oxley act (SOX) states that applicable business records must be stored and regulated for not more than a period of five years. However if the flow complies with the protocols of the network by matching the activity pattern, the will be considered as trusted flow that would earn its way towards the production server.

3.1.4 Relationship between Data Risk and Degree of Surety of a Secured Flow.

3.1.4.1 Risk associated with Data

It has been a continuous phenomenon that more and more information is transmitted and accessible via computer data networks. Therefore data networks become a critical spot with lots of risks and threats related to it. One example can be a temporary dysfunction of network caused by an intended attack (such as DDoS attack). Attacks may lead to server failures which can mean simple inability to provide required services but also they can paralyze systems on national level. Another possible risk associated with data would be the loss of credibility of data.

Crucial elements of data network can be overpowered by an attacker, for instance by breaking down password and setting administration access rights. Result of such activity can end up by

misusing the element of data network for illegal actions (e.g. phishing, Botnet) or by continuous abuse of the network.

Table 2: Following table provides a brief description of Risks associated with Data.

RISK	*DESCRIPTION*
Risk to loss of Data Integrity through mismatch of Job Profile.	These risks are mostly concerned with the loss of data credibility through a mismatch of expectations, for example not satisfying the criteria of pattern matching and going against the role that the user is assigned to. For any unexpected changes in the system can put data in the network at risk.
Risk due to storage of sensitive data in the database that could be vulnerable in case of attack.	These risks are concerned with storage of valuable information in the network database required for authentication purpose. No process involved to review the mechanism that would delete the user authentication data from the network database and store it in the encrypted log directory for network's future use can leave the network system assailable to a threat.
Risks of loss of data authenticity.	These risks are concerned with the loss of ability to track and record the origins of user data and the related operations performed on that data.
Risks of data degradation.	The risk associated with data degradation would be loss or damage of information due to an invasion on the network where the corrupt user tries to steal the valuable data from the network.
Risks to data through loss of services.	If there is a loss or interruption to the services and processes that are involved in preservation of data, then this has the potential to put the content itself at risk of loss. For example, this might be the loss of a service that routinely checks and monitors data flow within the network.

3.1.4.2 State of Art

Many systems used for a defense of cyber threats are based on the most common approach known as Deep Packet Inspection (DPI). Deep Packet Inspection approach consists in analysis of packet arriving from the source and passes only those packets to the destination that proves their identity to the network.

3.1.4.2.1 Deep Packet Inspection (DPI) Protocol

Deep Packet Inspection is a form of computer network packet filtering that examines each packet of information as it arrives from the source(client) and passes an inspection point(firewall) to search for any protocol non-compliance, intrusions or predefined criteria to decide if the packet can pass(directly to the Operating System) or if it needs to be routed to a different destination(Honeynet) for further analysis. DPI combines the functionality of an Intrusion Detection System (IDS) and an Intrusion Prevention System (IPS) with a traditional Stateful firewall. This firewall keeps track of the state of network connections such as TCP streams, UDP communication and is programmed to distinguish legitimate packets for different types of connections. Only packets matching the active connection will be allowed to pass through, others will be rejected. A Stateful firewall is able to hold significant attributes of each connection in memory, from start to finish. These attributes include IP addresses involved in the connections and the sequence numbers of the packets traversing the connection.

The combination of two functionalities (IDS/IPS and Stateful Firewall) makes DPI possible to manage the flows (packets, email or documents from the source) and detect any malicious, virus spreading entity entering the system.

DPI fulfills 2 different security related 'function' depending on the context where it is used:

1) Content inspection

In this context DPI looks for any virus or malware signatures that could be embedded in flows in addition to, specific patterns that should match against a list of known activity pattern. This is done using pattern matching algorithms and regular expression functions.

2) Network Analysis

In this context DPI is used to identify protocol and applications used on a network. This requires pattern matching, but also more complex protocol grammar analysis and statistical analysis.

Table 3: The chart below shows the difference between the 2 categories of DPI implementation[8]

	Content inspection	**Network Analysis**
Method	DPI: Inspect content of flows with its header.	
Objective / features	Detects malicious activity within the documents.	Recognize & analyze protocols and Applications.
How it works	Detect patterns	Multiple algorithms used such as pattern matching and behavior analysis.
Implementation	IDS/IPS	Forensics, Firewall

[8] Based on blog "Network Intelligence Technology-Deep Packet Inspection"

3.1.4.2.2 Network Behavior Analysis (NBA)

The concept of Network Behavior Analysis is introduced in this thesis to ensure guarantee of only known flow to be routed towards the production server. Network Behavior Analysis (NBA) is a way to enhance the security of a proprietary network by monitoring traffic and noting unusual actions or departures from normal operation.

A good NBA program can help a network administrator minimize the time and labor involved in locating and resolving problems. It should be used as an enhancement to the protection provided by the network's firewall, intrusion detection system, antivirus software and spyware-detection program[9].

NBA is commonly used in combination with anti-virus, anti-malware, IDS/IPS and other security technologies. Figure (9) shows the percentage usage of NBA in each security technology.

A combination of both methods-DPI and NBA, ensures a higher ability of system to react on a wider scope of threats and therefore increases security of a network in general.

3.1.4.3 Surety of Flows using these Approaches

There are a plenty of network security related issues. None of the approaches mentioned could be a fool proof for any system. For professionally prepared attacks coming from inside the network, the DPI results of analyzing the packets are significantly less powerful as there are constraints while dealing the contents of packets. The methods of payload analysis are very

[9] Based on urlhttp://searchsecurity.techtarget.com/definition/network-behavior-analysis

demanding for network performance and cannot be used in encrypted traffic while the ratio of encrypted traffic is increasing.

The following table shows an example of utilization of DPI and the NMA approaches for various task related to network security.

Table 4: Different tasks related to security using DPI and NBA methods[10]

Task	Deep Packet Inspection	Behaviour Analysis
Application protocol analysis	**YES**	**NO**
Signature-based IDS	**YES**	**NO**
Peer-to-peer networks	**YES**	**YES**
Dictionary attacks detection	**NO**	**YES**
Host profiling	**NO**	**YES**
Unknown threats	**NO**	**YES**

These tasks involve checking of flow specific pattern to detect particular network service or an activity. Some characteristics of related flows use Deep Packet Inspection as an approach to check the pattern, while some are checked by Behavior Analysis. These methods have large potential to complement a traditional signature-based approach. The key to guarantee a secure flow is a combination of DPI and NBA signature based detection methods.

[10] Based on article "From Signature-Based towards Behavior-Based Anomaly Detection(Extended Abstract)"

3.1.5 Pattern Matching

Pattern Matching is an important task in various applications, including network traffic analysis and intrusion detection[11].This thesis makes use of activity patterns to match a pre-defined set of activities with the flow activities and help untrusted flows to either earn their way in becoming trusted ones or terminate their connection with the network.

Matching a pattern of activity helps identify abnormal network activities within the network. This method observes the flow activity and records all malicious, unintended activities to be flagged based on a role ascribed and any mismatch of activity pattern.

3.1.5.1Port matching

In order to launch an attack on the network, the malicious user will target a specific, functional port to be compromised. For example, a user triggering an SQL Slammer worm works on port 1434 or the Netbus Trojan on port 12345. Network administrator filters all the flow records in order to find the corresponding attacks.

3.1.5.2 IP Address Matching

IP address is a way to identify flows in a whitelist or in a non-whitelist category. Following describes a way to make an IP address match:

IANA (Internet Assigned Numbers Authority)

The IANA has reserved large blocks of Internet address space which should not be used for global routing. If we find any flow record containing IANA reserved addresses, an alert should be triggered.

[11]Based on article "Hardware Pattern Matching for Network Traffic Analysis in Gigabit"

A check on corresponding router number in the flow records is essential to find the actual router interface where the flow comes from.

3.2 Comparison with Existing Methods

In the following section we will examine the traditional methods for achieving the goals set out in the flow analysis framework, how they operate and a discussion on their pros and cons will be presented.

3.2.1 Software Methods

3.2.1.1 Biometrics

Authentication by biometric verification is becoming increasingly common in corporate and public security systems, consumer electronics and point of sale (POS) applications. In addition to security, the driving force behind biometric verification has been convenience. However one of the problems listed by Churchward states that biometric data is inherently flawed choice for a primary method of authentication due to its uniqueness. Churchward says, “Once you have your fingerprint scanned it will give a unique data sequence which if compromised is not exactly something you can change. Imagine having an option of only one password 'ever'. One loss and you are screwed."Biometrics has failed to prove its existence in the theory of authentication due to factors like, the scanner not being able to recognize a real fingerprint on the machine, or to housebreak fingerprints using crime detection techniques.

Biometrics shares goal very much essential for authenticating data flow and will likely change as the technology evolves, but for now the system is still fallible, and not suitable to be a primary solution to the authentication problem[12].

3.2.1.2 SSH

SSH (Secure Shell) is an invention of a private company, aimed to provide secure access to network services such as file transfer or remote execution of processes. SSH key authentication works without passwords and involves a matched pair of keys (public and private) which when matched proves the identity of the source. This greatly reduces the risk of remote exploits such as password cracking utilities and brute force attacks against common or known accounts on a system. The password can be removed altogether as long as keys are the only method used for authentication. However it is likely that an account gets compromised that contains keys and is able to use the key pair to access accounts on other systems that is deemed unwanted access. Managing these keys within the stored files is a challenging job. Any given account can have multiple key pairs that are spread out through many systems. This makes it difficult to identify which keys are used on what servers.

The SSH protocol generally doesn't operate with anything useable like X.509 certificates. The only thing the server has is a key pair which is not quite sufficient to be considered as secure. The validation process is done using OnKeyValidate event of SSH/SFTP client components of SecureBlackbox. The client can show key's hash to the user, or check the key database or perform some other action to decide if the key is valid.

[12] Based on "Pros and cons of biometric authentication" at url http://www.net-security.org/secworld.php?id=8922

3.2.2 Hardware Methods

With the amount of security breaches along with the identified thefts and phishing attacks increasing, most of the companies worldwide have invested in reliable hardware authentication devices that offer enhanced network security. Frost & Sullivan Research Analyst Zubin Baben states the significance of hardware authentication devices by emphasizing the usage of 2-factor authentication approach to enhance network security. The benefit of utilizing the 2-factor authentication hardware device approach is that they serve the users' identity organizer managing their credentials whether they are encryption keys or passwords on one device. This eliminates the need to remember several different passwords to access different resources in the network.

Hardware devices usually have challenges in integrating the technologies with the existing IT infrastructure of the enterprise. Moreover, large-scale deployment requires backend software support and suitable infrastructure that may shrink the IT budget. Large companies are hoping for a comprehensive solution that will integrate physical and logical authentication processes in a user-friendly manner while simultaneously performing a variety of operations such as payment and employee benefits. *[Kim, D.-W., Kim, G. W., Lee, J.-H., & Han, J.-W, 2005]*

3.2.3 Comparison Summary

In summary, the existing methods offer quick and efficient means of handling the authentication process for the network. However with traditional approaches like single or a two-factor authentication, it becomes essential to maintain the passwords and encryption keys, failure of which might lead to the devastation of network database threatening enterprises' security. The

network security model proposed in this thesis is not based on one password or keys, but possesses an approach[13] designed to evaluate flows based on their job profile by matching patterns against the expected activities and filtering the known flows based on amenability of network's protocol. This helps not only in true ratification, but also justifies their integrity corresponding to their pattern of job activity.

[13]" Network Behavior Analysis: Protecting by Predicting and Preventing" at url: http://www.globaldataguard.com/downloads/Aberdeen_Research_Brief_NBA.pdf

Chapter 4 Summary

4.1 Conclusion

Using the concept of role and activity pattern, this framework is able to differentiate trusted flows (that match a whitelist or patterns of interaction) from the untrusted ones (that do not match the patterns) and supply resources available for use only to those who authorize themselves to the system by matching the pattern criteria corresponding to their role.

Security is not a patch which is to be implemented and forgotten. With the advent of large scale use of Internet, it is necessary to constantly update new events occurring. The administrator cannot afford to be left behind with the knowledge of upcoming security services, else might lead to the failure of network if the information falls into the hands of wrong person, bearing a potential threat to the enterprise.

4.2 Recommendation

The use of role in combination with the pattern matching should be implemented to help organizations be aware of flow's hustle within the system. In any case, if the encrypted database log gets exposed, it becomes vulnerable causing hazardous situations, thereby diminishing the protection policy applied to the network.

The network administrator should constantly make relevant security updates to the server to avoid any potential loss of data during any aberrant activity by a user.

The one location where the integrity of an entity will be preserved is at the server side; hence precautionary measure should be taken at a higher priority level to safeguard the valuable assets of the network.

Chapter 5 Future Work

The information presented in this thesis offers a variety of ideas regarding the future development of secure processing of traffic. Several suggestions for future research are presented to provide worthwhile ideas to pursue.

5.1 Refined Log Directories

In future iterations of this model, it would be beneficial to refine the use of a log directory for further observance in the production server. There will be no track kept of the activity that the flow performs, once it is admitted to the production environment. The logs will have a certain time frame to retain a check on movements, until the time frame runs out. Hence an enhanced logging system should be incorporated to view the activities of the flow after providing access to the production system.

5.2 Data Recovery

During the data recovery process, often the data is being salvaged from storage media such as internal or external devices. Recovery may be required due to physical damage to the storage device or logical damage to the file system that prevents it from being mounted by the host operating system. The most common "data recovery" scenario involves an operating system failure, in which case the goal is simply to copy all wanted files to another disk.

A scenario involves, where an illegitimate flow gets his hand on the substantial information leading to the access of company’s database, there should be some way to recover the lost data to bring up the abstracts on track and cut down the flow’s connection that caused this loss.

5.3 Roll-Back System

Rolling back means undoing changes to data that have been performed within an uncommitted network transaction. If at any time, a flow commits and unauthorized transaction into the network causing an error, all the transactions carried by the flow are rolled-back to the source at the connecting point to re-authenticate the flow for future connection with the network.

5.4 Improved Hardware and Software Methods

Investigation of tamper-resistant hardware methods for automatic verification of flow credentials may prove extremely useful in advancing this network security model. Utilization of Network Inspection System (NIS) software detecting vulnerability in a product and disclosing it on web might prevent attackers from compromising the network system.

Works Cited

Wikipedia. (n.d.), Retrieved from http://en.wikipedia.org/wiki/Main_Page (April 2011)

Configuring Role-Based Access Control (2010, October).*Cisco Application Control Engine Module Getting Started Guide*. Retrieved from http://www.cisco.com/en/US/docs/interfaces_modules/services_modules/ace/vA4_1_0/configuration/getting/started/guide/rbac.pdf.(April 2011)

Griffiths, M. E. (June 2007). *Patterns of User Activity in the Blackboard Course Management System Across All Courses* (Master's thesis, Brigham Young University, Rexburg).Retrieved from Brigham Library database. (May 2011)

Holland, T. (2004, February 23). SANS Institute Info Sec Reading Room. In *Understanding IPS and IDS: Using IPS and IDS together for Defense in Depth.* Retrieved from http://www.sans.org/reading_room/whitepapers/detection/understanding-ips-ids-ips-ids-defense-in-depth_1381 (April 2011)

Kim, D.-W., Kim, G. W., Lee, J.-H., & Han, J.-W.(2005). World Academy of Science, Engineering and Technology 8.In *Role-based Access Control Model in Home Network Environments.* Retrieved from http://www.waset.org/journals/waset/v8/v8-18.pdf (July 2011)

Mosse, F. G. Object Discovery In *Modeling Roles: A practical series of Analysis Patterns*, Retrieved from Google database (June 2011)

NIST/ITL Bulletin (1995, December).*An Introduction to Role-Based Access Control*. Retrieved from Wikipedia database. (May 2011)

Shuja, F. A. (2004, March 5). Honeynet. In *Pakistan Honeynet Project*. Retrieved from http://www.Honeynet.pk/Honeynet. (April 2011)

Potter, B. (2008). *Network Flow Analysis*. Retrieved from DefCon website: http://www.defcon.org/images/defcon-16/dc16-presentations/defcon-16-potter.pdf(Sept 11)

Tollet, J. (2011, September 16). Deep Packet Inspection: don't mix-up content inspection and network analysis [Online forum message]. Retrieved from Network Intelligence Technology: http://networkintelligence.blogspot.com (Sept 2011)

Gong, Y. (2010, November 2). Detecting Worms and Abnormal Activities with NetFlow, Part 1 [Web log post]. Retrieved from Symantec: http://www.symantec.com/connect/articles/ detecting-worms-and-abnormal-activities-netflow-part-1 (Oct 2011)

Maier, G. M. (May 2007). *Hardware Pattern Matching for Network Traffic Analysis in Gigabit* (Master's thesis: Technical University of Munich, Munich). Retrieved from http://www.icir.org/gregor/papers/diplomarbeit.pdf. (Oct 2011)

Minarik / Vykopal, P. /. J. (2010).*From Signature-Based Towards Behavior-Based Anomaly Detection* (Master's thesis, Minarik University, Brno, Moravia, Czech Republic). Abstract retrieved from http://ftp.rta.nato.int/ public//PubFullText/RTO/MP/RTO-MP-IST-091///MP-IST-091-P02.doc (Oct 2011)

Addis, M. (2010).*Threats to data integrity from use of large-scale management environments*. Retrieved from Presto Centre website: http://www.prestocentre.eu/system/files/Threats%20to%20data%20integrity_v1.0.pdf(Oct 11)

Greer, C. (2011, August 4). Packet Capture vs. Flow Collection: Which one do I need in a monitoring solution? [Online forum message]. Retrieved from Packets in Paradise blog: http://myaccount.flukenetworks.com/fnet/en-us/ Community/ Packets_in_Paradise?plckPostId=Blog%3A1d69ff7a-abce-4694-9d65-915308c354a3Post%3A 0590cc72-e646-4813-9ce2-a8bfcdf77cce&plckController=Blog&plckScript=blogScript&pl ckBlogPage=BlogViewPost&plckElementId=blogDest(Sept 2011)

Network Behavior Analysis (NBA).(2006, October). Retrieved from http://searchsecurity.techtarget.com/definition/network-behavior-analysis (Oct 2011)

Aberdeen Group. (2009). *Network Behavior Analysis: Protecting by Predicting and Preventing*. Abstract retrieved from http://www.aberdeen.com/ website: http://www.globaldataguard.com/downloads/Aberdeen_Research_Brief_NBA.pdf (Oct 2011)

Sutherland, L.-P.(1998, October).Biometrics [Web log post]. Retrieved from Search Security: http://searchsecurity.techtarget.com/definition/biometrics November (2011)

Zorj, Z. (2010, February 26). Help Net Security. Pros and cons of biometric authentication. Retrieved from http://www.net-security.org/ secworld.php?id=8922 November(2011)

SSH Authentication methods. (n.d.). Retrieved from Eldos Corporation website: http://www.eldos.com/security/articles/1962.php November (2011)

Zambrana, S. (2008, November). Secure shell [Abstract]. In SSH Key Authentication (ISC-SEO ed.) November (2011)

IT & Security Portal. (2005, September 30). Hardware authentication devices are secure. [Web log post]. Retrieved from http://www.it-observer.net/ November 5 (2011)

IBM-AIX 6.1 Information.(n.d.).RBAC roles. In *AIX-Advanced Interactive eXecutive*. Retrieved from Google database. March (2012)

jayrulez. (2010, March 4). RBAC - set multiple roles for user? [Online forum message]. Retrieved from http://www.yiiframework.com/forum/index.php/topic/7669-rbac-set-multiple-roles-for-user/ March (2012)

Glossary

Source A computer in a network that uses the services (as access to files or shared peripherals) provided by a server [MW].

Server Any combination of hardware or software designed to provide services to clients [WP].

Flow A sequence of packets from a source computer to a destination, which may be another host, a multicast group, or a broadcast domain [WP].

Packet A formatted unit of data carried by a packet mode computer network [WP].

Data An information in a numerical form that can be digitally transmitted or processed [MW].

Data Breach The unintentional release of secure information to an insecure environment [WP].

Computer Network A collection of hardware components and computers interconnected by communications channels that allow sharing of resources and information [WP].

Network Traffic A data in a network. In computer networks, the data is encapsulated in packets [WP].

Encryption A process of transforming information (referred to as plaintext) using an algorithm (called cipher) to make it unreadable to anyone except those possessing special knowledge, usually referred to as a key [WP].

Production Server A system that acts as an interface between hardware and user; the production server is responsible for the management and coordination of flow activities and the sharing of the resources of the computer [WP].

Authentication A mechanism whereby systems may securely identify their users. Authentication systems provide answers to the questions:

- Who is the user?
- Is the user really who he/she represents himself to be? [WP]

Authorization A mechanism by which a system determines what level of access a particular authenticated user should have to secure resources controlled by the system [WP].

Router A device that forwards data packets between computer networks, when data comes in on one of the lines, the router reads the address information in the packet to determine its ultimate destination [WP].

Covert Network A network set up with intentional vulnerabilities to invite attack, so that an attacker's activities and methods can be studied and that information used to increase network security [WP].

RBAC An approach to restricting system access to authorized users [WP].

Role A prescribed or expected behavior associated with a particular position or status in a group or organization [WP].

Activity Pattern A profile of activities needed to follow in order for the user to earn its way out of Honeynet.

TCP Provides reliable, ordered delivery of a stream of bytes from a program on one computer to another program on another computer [WP].

IDS A passive device watching packets of data traverse the network from a monitoring port, comparing the traffic to configured rules, and setting off an alarm if it detects anything suspicious. [WP].

IPS A network security appliance that monitor network and/or system activities for malicious activity [WP].

DPI A form of computer network packet filtering that examines the data part of a packet as it passes an inspection point, searching for protocol non-compliance, viruses, spam, intrusions or predefined criteria to decide if the packet can pass or if it needs to be routed to a different destination[WP].

NBA A way to enhance the security of a proprietary network by monitoring traffic and noting unusual actions or departures from normal operation [WP].

Access Control A computer security network approach that attempts to unify endpoint security technology, user or system authentication and network security enforcement [WP].

IANA IANA Responsible for the global coordination of the DNS Root, IP addressing, and other Internet protocol resources [MW].