SiDR: A SECURE INTER-DOMAIN ROUTING PROTOCOL FOR FUTURE INTERNET

A Thesis
IN
Computer Science

Presented to the Faculty of the University
of Missouri–Kansas City in partial fulfillment of
the requirements for the degree

MASTER OF SCIENCE

by
CHOCKALINGAM ESWARAMURTHY

B. Tech., SRM University, Chennai, India, 2007

Kansas City, Missouri
2011

SIDR: A SECURE INTER-DOMAIN ROUTING PROTOCOL FOR FUTURE INTERNET

Chockalingam Eswaramurthy, Candidate for the Master of Science Degree

University of Missouri–Kansas City, 2011

ABSTRACT

Inter-domain routing is a critical functionality that help connect autonomous systems in the Internet. In recent years, there have been concerns in regard to its vulnerabilities such as IP prefix hijacking and worm attacks. Many of the problems in the inter domain routing arises from the protocol complexity, lack of support for underlying policies, vulnerabilities, convergence and route stability, scalability and isolation. A number of approaches have been proposed to address the known vulnerabilities.

In this work, we propose an inter-domain routing protocol for future evolution of the Internet. Our approach, SiDR (Secure inter Domain Routing Protocol), addresses security and benefits from novel technique such as Attribute Based Cryptography (ABE) for achieving policy routing and information hiding. SiDR offers a new perspective and direction for discussions on inter domain routing. We focus on two aspects of inter domain routing that is of paramount importance; routing policies and security.

APPROVAL PAGE

The faculty listed below, appointed by the Dean of the School of Computing and Engineering, have examined a thesis titled "SiDR: A Secure inter-Domain Routing Protocol for Future Internet," presented by Chockalingam Eswaramurthy, candidate for the Master of Science degree, and hereby certify that in their opinion it is worthy of acceptance.

Supervisory Committee

Deep Medhi, Ph.D., Committee Chair
Department of Computer Science & Electrical Engineering

Lein Harn, Ph.D.
Department of Computer Science & Electrical Engineering

Yugi Lee, Ph.D.
Department of Computer Science & Electrical Engineering

CONTENTS

ILLUSTRATIONS

ACKNOWLEDGEMENTS

I would like to thank my academic advisor Dr. Deep Medhi for his guidance during my thesis research. This thesis work is my first research, and Dr. Medhi gives me a valuable mentoring from finding a research topic to writing papers. On the other hand, I would like to thank Dr. Lein Harn and Dr.Yugi Lee from Department of Computer Science and Electrical Engineering for their advice on my thesis work.

I would like to thank my lab mates at the Computer Networking Research Laboratory (CoNReL) for their discussion and critiques.

Furthermore, I would like acknowledge my entire family for their support and encouragement during the whole study of my master study.

CHAPTER 1

INTRODUCTION

Internet was designed for transmitting data from point A to point B as a best effort scheme. After almost 40 years, the core design of the Internet remains the same, but the demands of the Internet usage have been drastically changed. Future Internet design is a hot area of research today as researchers try to understand the dynamics and demands of todays' Internet and predict the demands of future Internet thereby proposing novel framework and protocols that meet those demands. Today Internet relies heavily on the inter-domain routing to make communications happen on the Internet. The most popular inter-domain routing protocol is the Border Gateway Protocol. Another protocol in the Asynchronous Transfer Mode (ATM) world is Private Network-to-Network Interface (PNNI). PNNI is a hierarchical state-of-art routing protocol and is known to use Quality-of-Service sensitive routing scheme by advertising topology state parameters and Call Admission Control [1] .

Recent turn of events and studies have shown that the present inter domain routing have a number of security vulnerabilities. Some of the commonly know threats are: (a) the nodes are vulnerable to active and passive wiretapping attacks, (b) a node may be compromised, and (c) Configuration information or routing database of a node may be modified or replaced via un-authorized access to a router or server or via a spoofed distribution channel. There has been several efforts to to negate these problems [13].

1.1 Overview of Inter Domain Routing and Security

At the heart of the Internet lies routing. Network Routing refers to the ability of an electronic communication network to send a unit of information from point A to point B by determining a path through the network, and by doing so efficiently and quickly [16]. Routing essentially involves the following operations, (a) exchange of routing information between different systems (routers) that participate in the process and (b) finding the optimal path from point A to point B. Internet is made up of many entities known as autonomous systems. These autonomous systems define the administrative authority and routing policies of different organizations. Autonomous systems work by running inter domain and intra domain protocols that communicate reachability information between themselves. The protocols that can are supported by a typical autonomous system are Border Gateway Protocol (BGP), Interior Gateway Protocol (IGP), Routing Information Protocol (RIP), Enhanced Interior Gateway Routing Protocol (EIGRP), Intermediate System-to-Intermediate System (IS-IS) etc. The standard exterior routing protocol that is used by the autonomous systems today is the BGP-4.

Exterior Routing Protocols were created to control the expansion of the routing tables and also separate out routing domains into independent administrative domains that can have their own routing policies.

Recent turn of events have shown that a number of security threats of the current inter domain routing has been exposed over the years thorough occasional accidents or misconfiguration and through extensive study and survey of the BGP protocol with respect to security. Murphy in RFC-4272 explained in detail the various vulnerabilities faced by

BGP. The main reason for this weakness is since BGP as a protocol does not define any cryptographic mechanisms for authentication of the peer to peer communication. Since BGP is dependent on TCP transmission for its functioning, BGP is vulnerable to all those vulnerabilities faced in such communication such as IP spoofing, session stealing, TCP SYN attack, and so on. A third party can inject malicious AS numbers unintentionally or intentionally into a BGP stream thereby creating a havoc in the entire network. Some of the real world scenarios of such attacks would be the YouTube.com outage that occurred in February 2008 [19] and China Internet Hijacking in April 2010 [17]. A list of the known security threats of BGP as discussed in RFC-4272 can be classified as follows:

- Confidentiality Violation: The routing information present in BGP is in plain text, hence it is vulnerable to eavesdropping and easy to plan attacks.

- Replay: BGP as a protocol cannot distinguish between current BGP messages and replayed BGP message from previously recording activity.

- Message Insertion/Deletion/Modification: BGP protocol does not have a mechanism to prevent a BGP message from being manipulated in any way by a genuine BGP speaker or a hacker.

- Man-in-the-middle attack: As there is no authentication mechanism in BGP protocol; it is easy to capture a packet, to modify it and to send it to the destination thereby diverting and extracting vital information from between the communicating parties.

- Denial-of-Service (DoS): Another widely seen attack is DoS attack. Because of today's rapid growth in technologies and low-cost infrastructure, it is easy to design and develop such a attack at massive scale. Due to the in-availability of proper authentication mechanism, BGP is unable to stops such attacks.

Further vulnerabilities of BGP were exposed by Hu et. al. in [10]. The classification of threats is as follows:

- Falsification Attacks: Modification or false advertising a route in a BGP message is termed as falsification attack. Examples include falsifying the withdrawn route, falsifying a Network Layer Reachability Information (NLRI), falsifying path attributes, truncation, and so on.

- Wormhole or tunnel: Another type of attack is a wormhole or tunnel. This specific mechanism creates a black hole in the network. Any information that goes into the black hole is essentially lost in there which can result in a major increase in the traffic of the network and can result in the phenomenon similar to the YouTube.com outage mentioned earlier.

- Unauthorized AS path announcements: A hacker can intentionally announce prefixes that are not supposed to be announced as per policies of the ISP. This increases the overall traffic in the network, causing congestion, and performance degradation.

1.2 Problem Definition

The goal of our work is to propose a novel protocol SiDR for securing the inter domain routing and communication in the future Internet. Briefly, we use Attribute Based Cryptography for securing the inter domain routing updates.

Inter domain routing presents a challenging task of policy, security and algorithmic properties to be satisfied. It has become highly aware that routing policies are a matter of serious concern in the inter domain routing design space. The IRTF and SIDR working groups have put together a set of requirements to be considered while designing a future inter domain routing protocol [20]

From this non-exhaustive list of specifications we chose two design constrains for designing SiDR, namely: (a) Policy routing: A future inter domain routing must support policy routing by design. By this it is possible to avoid highly mysterious and onerous ways of configuring policies and its decision processes. (b) Security : Information hiding is a crucial design requirement for any protocol today. The inter domain routing information exchanged between systems today make the Internet vulnerable to localized security or misconfiguration.

1.3 Related Work

In this section, we will briefly discuss the current literatures.

Today the widely used inter domain routing protocol is Border Gateway Protocol (BGP). Recent turn of events have shown BGP being vulnerable to various types of attacks

and over the years, a number of approaches have been proposed to address the security issues associated with the current inter-domain routing protocol namely, BGP. Events such as the YouTube.com hijacking [19] and Internet hijacking [17] have a got topic of discussion recently. Heffernan proposed to protect BGP sessions via TCP MD5 signature option RFC-2385. Ferguson and Senie RFC-2827 proposed to use network ingress filtering to negate denial of service attacks which employ IP source address spoofing. Geofferey et al proposed the Inter domain Route Validation (IRV) service to work around BGP by introducing a receiver based protocol that works in parallel with BGP to give feedback to the sender about a UPDATE message [9]. IPSec has also been proposed to secure BGP sessions. While IPSec is not specific to BGP alone, it is a protocol stack to secure communication between two entities. A list of approaches has been summarized in the BGP survey paper [7].

Secure-BGP was the first proposed architecture to solve the security issues with BGP [14]. S-BGP employs three security mechanisms: (a) A public key infrastructure that parallels the IP address and AS number assignment to enable authentication of ownership of IP address blocks, autonomous system numbers, AS identity and BGP router's identity, (b) S-BGP added a new attribute path called the BGP transitive path attribute to carry the digital signatures; this is used for attestation purposes and (c) IPSec was proposed to be used to provide data communication integrity. The goal of S-BGP was to achieve the correct operation of BGP as defined in the S-BGP proposal.

Secure Origin BGP (soBGP) is another mechanism for securing the border gateway protocol [22]. soBGP followed schemes such as S-BGP, Internet Route Verification,

and DNS- based Network Layer Reachability Information (NLRI) origin AS verification in BGP [2]. The main goals of soBGP were quite similar to those of the S-BGP. soBGP proposed to separate the authentication mechanism from the core BGP processing. soBGP assumes that the security between two BGP speakers are addressed through mechanisms like BGP MD5, GTSH. soBGP was more concerned with securing the information within BGP using certificate mechanisms. It proposed protocol extensions [SOBGP-BGPTRANSPORT], [SOBGP-CERTIFICATE], [SOBGP-RADIUS] and certificates EntityCert - that ties an AS number to a public key, AuthCert - that ties an AS to a block of addresses that a AS may advertise. soBGP separated out the adjacency between devices running the routing protocol and the information carried within the routing protocol and hence, this requires additional cryptographic devices to perform the authentication process. From the certificates and BGP UPDATE messages each AS builds a AS connectivity graph using that future UPDATES can be validated.

Secure Path Vector protocol [10] is an innovative increment of the original S-BGP. SPV is a new protocol to secure BGP UPDATE message. The broader goal of the SPV protocol was to achieve incremental benefits with minimal changes to existing code. However, there are some limitations for most practical security mechanism to detect all BGP security failures, for example, handling of Byzantine failures are difficult. Since each AS can potentially *change* the content of update message or change the policy simply because it does not want to forward a particular AS number as per their local policy. In such cases, it is difficult to identify if a router is functioning properly. SPV proposed to use symmetric cryptography, replacing the asymmetric cryptography in S-BGP. It was

then shown that the performance of the algorithm speeds up by *22 times* when compared to S-BGP.

An important goal of SPV was to achieve ASPATH integrity through purely symmetric functions. A new cryptographic construction was introduced known as ASPATH Protector to achieve ASPATH integrity. The concept of epochs of fixed length and periodic updates to prevent replay attacks was also introduced. SPV proposes to use four different types of private and public keys namely (a) single ASN public/private keys - used to authenticate signature of one AS in ASPATH, (b) Epoch public key, (c) Multi epoch public key, prefix public/private key - standard RSA algorithm used and the prefix private keys are to be distributed by the ICANN.

SiDR loosely builds upon another work that explores a new link state protocol for securing the inter-domain routing [12]. This architecture explains the various attacks possible on a BGP protocol and presents a design for building a secure network. The major difference between SiDR and this architecture is that we consider the secure protocol from a policy aspect point of view. Being able to embed policies in a inter-domain protocol is a very important feature as it solves many problem from configuring a network to specifying access permissions. Another work that builds on the previously mentioned paper is [15]. In this work the authors present a detailed study of different types of attacks that are possible on a network and present a infrastructure for negating them. This work however does not capture the policy aspect of the network. SiDR not only encrypts the updates against various forms of attacks, it also gives the flexibility to specify network specific policies and also support dynamic domains.

1.4 Summary of Contributions

Our contributions are the following:

- We propose a new inter domain routing protocol for future Internet by leveraging on novel techniques like Attribute based encryption.
- We logically prove how the proposed architecture is robust against proven attacks.
- We present performance and security evaluation of the proposed protocol.

CHAPTER 2

ATTRIBUTE BASED ENCRYPTION

Attribute Based Encryption (ABE) is a novel idea of encrypting the information based on the attributes of the participating entities. This allows the flexibility of a dynamic environment and also has the added benefit of shorter key sizes compared to most the cryptographic algorithms available today. A number of approaches for ABE such a Cipher-Text policy based ABE, Multi-Authority ABE, Bounded CipherText ABE, Key-Policy based ABE have been previously proposed.

A central authority will create secret keys for the node based on its attributes/policies. Nodes in the system have attributes. They receive a key from an authority for its set of attributes. Ciphertext contains a policy (a boolean predicate over the attribute space). If a nodes' attribute set satisfies the policy, then it can use its key bundle to decrypt the ciphertext. For instance, the service provider may specify the following access structure for sending out route update based on a policy that the receiving entity should be a DSS (Dynamic Service System), and it should have a med value of 20 and action pref 1: (DSS AND med = 20 OR action pref = 1), by this, the service provider will be able to do policy routing. An access structure can be represented as a expression tree with the AND, OR operator at every node and the labels being the properties or attributes.

ABE benefits from its fundamental mathematical construction called Bilinear maps like other encryption methodologies such as Elliptic Curve Cryptography (ECC), Identity

Based Encryption (IBE) and Pairing Based Cryptography (PBC). It is important to note that the security and strength of ABE is based on the Decisional Diffie-Hellman problem [5]. A detailed analysis and proof for this can be found here [23]. A note on the performance of the ABE can be found here [4].

Attribute based encryption follows four fundamental algorithms; they are Setup, Encrypt, Key Generation, and Decrypt. We use the CP-ABE construction and algorithm as described in [4].

- Setup phase: During this phase, the master key is generated. The setup algorithm chooses a bilinear group $\mathbf{G^0}$ of prime order p with a generator g. It will choose two random exponents α, β, and Z_p. The public key generated is:

  PK = $\mathbf{G^0}, g, h = g^\beta$ and the master key is (β, g^α) The setup function is a two step process, it generates a public key and a master key which can be used with the encryption, decryption module and it generates private keys for each of the sub nodes.

- Encryption phase: The encryption algorithm takes the public parameters, message and access structure to produce the ciphertext CT. The ciphertext will also contain the access structure. CT is calculated using the formula:

  $CT = (\tau.\widehat{C} = Me(g,g)^{\alpha.s}, C = h^s, \forall \epsilon Y : \qquad C_y = g^{q_y(0)}, C'_y = H(att(y)^{q_y(0)}).$

  The input to this encryption function will be the public key generated in the setup step, the policy attributes and the message to be encrypted.

- c. Key generation phase: The key generation algorithm takes the master key and

the attribute sets to generate the private key SK. The formulation for the KeyGen algorithm is:

$$SK = (D = g^{(\alpha+\gamma)/\beta}, \forall \epsilon S : \qquad D_j = g^r.H(j)^{r_j}, D'_j = g^{r_j}).$$

- d. Decryption phase: The decryption algorithm takes the ciphertext and only if the recipient's attributes are satisfied by the access structure. The formulation used for decryption is:

$M = \widehat{C}/(e^{h^s, g^{(\alpha,\gamma)/\beta)}}/e^{(g,g)^{\gamma,s}})$ The DSS will use its private key obtained from the registration process from its parent DSD. The private key is basically a expression tree with the nodes being either logical AND or OR gates and the labels being each of the attribute of the DSS.

CHAPTER 3

SIDR DESIGN

Inter domain routing presents a challenging task of policy, security and algorithmic properties to be satisfied. It has become highly aware that routing policies are a matter of serious concern in the inter domain routing design space. The IRTF and SIDR working groups have put together a set of requirements to be considered while designing a future inter domain routing protocol [20] . From this non exhaustive list of specifications we chose two design constrains for designing SiDR. (a) Policy routing: A future inter domain routing must support policy routing by design. By this it is possible to avoid highly mysterious and onerous ways of configuring policies and its decision processes. Many of today's issues arise due to simple misconfiguration. (b) Security : Information hiding is a crucial design requirement for any protocol today. The inter domain routing information exchanged between systems today make the Internet vulnerable to localized security or misconfiguration. It is to be noted that a simple mis configuration can bring down the entire network.

We start this section by describing the structure of SiDR, support for policy routing and security features of SiDR.

The structure of SiDR is hierarchical by design. We introduce the concept of Dynamic Service Domains (DSD), Dynamic Service Systems (DSS) and super-Domains.

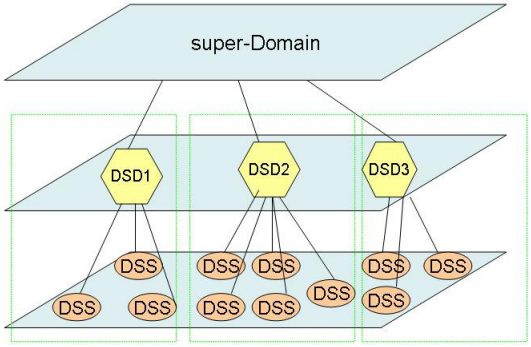

Figure 1: High level architecture

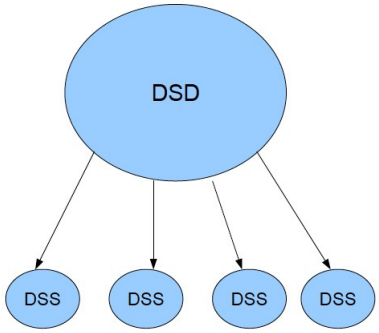

Figure 2: Relationship between a DSD and DSS

DSD's are networks owned and operated by single entity or institution. A DSS is a sub-system to a particular DSD. DSS can either be a virtualized entity or a physical entity. The concept of virtualized entities is explained in other work [11] . super-Domains are a level above the DSD's and are primarily concerned with setting up of global parameters or attributes for a DSD. We base our design leveraging on the existing hierarchical structure of ICANN.

Fig. 1 shows the high level routing structure of SiDR. Fig. 2 shows the relationship

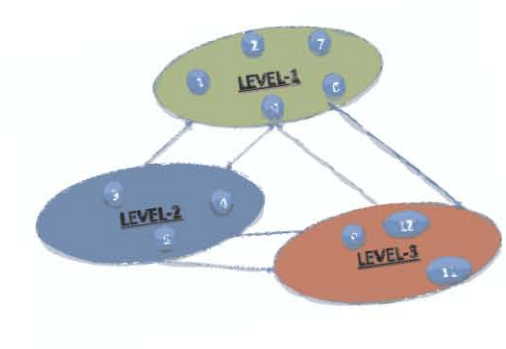

Figure 3: Domain Formation

between a DSD and a DSS. We illustrate an example of domain formation in Fig. 3

3.1 Policy Based Routing

Inter domain routing protocol has become inherently complex due to the incremental modification of the protocol by accommodating policies and decision processes. This has led to several problems, including unforeseen security vulnerabilities, widespread misconfiguration and conflicts betweens policies of different service providers. Today's Internet relies on service level agreements (SLA's) to be able to enforce policies for legal and financial reasons. SLA is a contractual agreement between a service provider and a service requester. However, it is critical to be able to enforce policy from a design perspective as well. In SiDR, we provide this ability for a DSD to configure the policy based on the attributes of a individual DSS. Attribute based encryption (ABE) becomes a natural suitor for achieving this requirement.

3.2 Security

SiDR leverages on Attribute Based Encryption for achieving information hiding requirement of inter domain routing protocol. Attribute Based Encryption (ABE) is a novel idea of encrypting the information based on the attributes of the participating entities. This allows the flexibility of a dynamic environment. A number of approaches for ABE such a Cipher-Text policy based ABE, Multi-Authority ABE, Bounded CipherText ABE, Key-Policy based ABE have been previously proposed.

ABE benefits from its fundamental mathematical construction called Bilinear maps like other encryption methodologies such as Elliptic Curve Cryptography (ECC), Identity Based Encryption (IBE) and Pairing Based Cryptography (PBC). The cryptographic technologies that are constructed from Bilinear Maps also have the advantage of smaller key sizes as when compared to other standard cryptographic algorithms and this vastly helps in improving the processing times. It is important to note that the security of ABE is based on the Decisional Diffie-Hellman problem [5] which makes it robust against various attacks. A detailed analysis and proof for this can be found here [23]. In our approach, we would like to use ABE mainly for securing the content, enabling levels of serviceability (Security) and to support the dynamic serviceability.

Attribute based encryption follows four fundamental algorithms; they are Setup, Encrypt, Key Generation, and Decrypt. We use the CP-ABE construction and algorithm as described in [4].

- Setup phase: Setup()

  The setup algorithm is run at the DSD, it takes no input other than the implicit security parameter. It outputs the public parameters PK and a master key MK.

- Key generation phase: Key Generation (MK, S_{DSS})

  The key generation algorithm is also run at the DSD, it takes as input the master key MK and a set of attributes S_{DSS} for a particular DSS that describe the key. It outputs a private key SK_{DSS} for a particular DSS. This step is repeated for each of the DSS that registers with the DSD. Thus generating key pairs for DSS and distributing it to them. The private keys are distributed to individual DSS's using Identity Based Encryption [6]. Public parameters for a particular DSS can be its attributes, for example DSSID, level of service etc.

- Encryption phase: Encrypt (PK, STATUS, Policy)

  The encryption algorithm takes as input the public parameters PK, the SiDR STATUS, and an access structure Policy over the universe of attributes. The algorithm will encrypt STATUS and produce a ciphertext CT_{DSS} such that only that DSD that possesses a set of attributes that satisfies the access structure Policy will be able to decrypt the message. We will assume that the cipher text implicitly contains Policy .

- Decryption phase: Decrypt (PK, CT_{DSS}, SK_{DSS})

  The decryption algorithm takes as input the public parameters PK, a ciphertext CT_{DSS}, which contains an access policy Policy , and a private key SK_{DSS}, which

is a private key for a set S_{DSS} of attributes. If the set S_{DSS} of attributes satisfies the access structure Policy then the algorithm will decrypt the ciphertext and return a message STATUS.

The DSS's exchange the STATUS message using the ABE encryption as described in the encryption phase.

CHAPTER 4

SIDR: PROTOCOL ANALYSIS

This section illustrates the proposed SiDR protocol information and packet format. Fig. 4, and Fig. 5 represents the different messages that gets exchanged. In Fig. 6 we show how the domains are formed based on policies and logical grouping by ABE. Let's assume level-1 has highest security, level-2 has medium security and level-3 has low security. The levels of security can either be chosen by a parent DSD or a super-Domain, or by using a distributed polling approach as that of the PGP mechanism. The level of security will be an attribute for each of the DSS and is obtained at the time of registration. It is important to note that the DSS belonging to different levels of security can be of the same network also as depicted in the example Fig. 6. If we want to change a policy and do a re-ordering of the logical group, we just need to change the "level" that we input to the ABE algorithm without any extra work or configuration.

The service providers can provide variable levels of security based on the levels. An example would be to have the government information classified as level-1 and when using ABE, level-1 would be a attribute to the algorithm. This also allows the classified information to remain as a separate domain at the high level even though they will be physically connected to other DSD's.

SiDR STATUS message is used to exchange information between different DSD's. The DSD STATUS message contains a aggregated route information of a list of DSS that

are accessible through that particular DSD. This message is exchanged between DSD's to obtain the connectivity information to various DSS's. Each DSD has a unique ID called the DSDID that is obtained from the super-Domain. The message format for this message is depicted in Fig. 4. Each DSS will have the a unique ID assigned by the DSD, this information will be communicated between individual DSS and DSD. Different DSD's are identified based on the level of service. The STATUS message is encrypted using ABE as per the policy specified by the transmitting entity. In order to validate the authenticity of the sender SiDR uses the digital signature mechanism in the protocol.

4.1 Basic Route Propagation model using Attribute Based Encryption

Based on the hierarchical routing structure of SiDR discussed in the previous section, we will use the simple path vector protocol along with ABE to achieve the dual goal of policy routing and information hiding.

The ABE-set up algorithm and ABE- key generation algorithm are run at entities higher in the hierarchy. Hence, the super-Domain generates the security keys and attributes for individual DSD's. The DSD in turn generate the security keys and attributes for individual DSS's belonging to them.

Each routing information exchange is encrypted using the encryption algorithm mentioned in the previous section. Similarly, every message received is decrypted using the decryption algorithm mentioned in the previous section.

In order to achieve policy routing, let us consider an example, suppose we want to

Route Info	Length	Type	Version

Figure 4: SiDR STATUS update format

Level Of Service	DSDID	NumOfDSS's	Signature

Figure 5: Route Information (Route Info)

DSSID	Level-of-Service	Signature

Figure 6: DSS-List Information

configure a policy for shortest path in today's router we specify say the local pref parameter equal to one and the multi-exit-discriminator to twenty. In SiDR, we can specify this policy as ('pref=1') and('med=20') as the policy string during our encryption phase.

Now suppose, we have another policy that only the DSS's local to a specific DSD should be able to decode the route information exchange, then we can pass the policy string (DSS and 'domain=local') as one of the inputs for the encryption algorithm. So only those entities that match the attributes will be able to decode the route information. By doing this we achieve information hiding by using the hierarchical structure of SiDR to avoid vulnerabilities like localized security or configuration problems. ABE policies can be written as a set of policies and is easy to configure and implement by the provider.

CHAPTER 5

EVALUATION AND DISCUSSION

We explain below the security evaluation of SiDR.

5.1 Logical Proof of Security

SiDR architecture is logically proved to be secure based on three assertions. They are:

1. Unique Identity Registration To join a DSD a particular entity has to obtain a pair of attributes and unique key pairs to take part in the network. Mechanisms such as those listed in the bootstrapping section can be modified and used here.

2. A distributed key generation/distribution approach Attributes and Key pairs obtained from a DSD will not be valid under another DSD unless transferred properly.

3. Breaking a Bilinear construction is Decisional Diffie-Hellman problem The security and strength of SiDR is based on Decisional Diffie-Hellman Assumption and breaking its construction is considered a Decisional Diffie-Hellman problem.

Property 1 assures that every DSS is uniquely identifiable. Consider a Man-in-the middle scenario, any third party in-order to participate in the network will have to go through the registration process to obtain the attributes and key pairs. Without these it cannot participate inside the DSD. We assume there is also a off line verification mechanism to register the identity and hence is traceable. Without the attributes and key pairs

it is difficult for a third party to act as another DSS. Even if it does forge the attributes, without the access structure and key pairs its not possible to decrypt the message. Hence, based on our assertions, we show that SiDR is resistant to third party attacks. Unless a entity is a ”registered” part of the network, there is little possibility of performing attacks such as modifying a STATUS message of SiDR or inserting false routes into the STATUS message, thus making it secure by design. Property 2 assures that a third party cannot obtain or forge a key pair without having the appropriate attributes to participate in the process. Property 3 assures that cryptanalysis techniques will lead to the Decisional Diffie-Hellman problem which is mathematically considered not solvable.

There is however a possibility of insider attack, which require further study to strengthen the protocol. Lets' take the case of a compromised DSS, if a hacker somehow gains access into a DSS, he will gain access to the attribute set and key pairs. This will enable him to perform attacks like sending out invalid routes and creating a blackhole. However it should be noted that a insider attack is ”traceable” because of its unique identity which makes it easier for administrators to track the source of attack and fix it.

5.2 Performance Evaluation

In this section, we discuss the performance of SiDR and contrast with SPV. We chose to compare and contrast with SPV because SPV is considered to be the most efficient secure inter domain protocol available and a comparison would give us a fair idea of how well SiDR performs.

We evaluate the security and efficiency of SiDR and compare it with the Secure

Path Vector Protocol [10] . We first give the logical proof of security of SiDR and then analyze the performance of the encryption methodology used.

For performance evaluation, we have collected data from the Oregon Route View Server for the day Sunday, 24 February 2008. This was the period when YouTube.com was hijacked on a global scale and went down for several hours. We chose this data to best reflect the heavy usage pattern of the routing protocol. In order to understand the behavior of the protocol under normal circumstances, we chose two additional datasets 8 months apart before and after the YouTube.com hijack incident.

In order to understand the diversity of the YouTube.com hijack data set, we present some of its facts obtained using a simple script below:

1. There were about 260671 different prefixes that appeared in the data.

2. About 27762 different AS numbers appeared in the data.

3. At this time there were about 65184 different AS-AS connections.

SPV is built upon Rijndael block cipher with a 128-bit key and a 128-bit block size, so we chose to use Advanced Encryption Standard 128 bit which is also based on Rijndael block cipher for a comparison. The ABE toolkit was obtained from [3] . The security of ABE algorithm is based on Decisional Diffie-Hellman assumption and breaking it is considered mathematically unsolvable.For evaluation purposes, we consider two cases first the extreme case which is the YouTube.com hijack scenario and the normal case which is the dataset collected on a time without any specific outage or attack. Fig. 7, Fig. 8 shows the times taken for encryption and decryption of the extreme case inter

domain routing data dump from the Oregon route view server for SPV and SiDR. The BGP-4 spec defined in RFC 4632, the smallest BGP data that can be in any network is the BGP header alone without any data is 19 bytes in size. The biggest BGP packet to be supported by any router in the network is about 256kb in size. The three datasets, the Full Data, Half Data and Quarter Data are provided solely for analysis purposes to test the extremeness of each algorithms. But in a real scenario, a specific node will not process data of sizes bigger than 256KB at a given time.

As mentioned before, we obtained three different datasets from Oregon route views server as mentioned in the above section. Each operation (encryption / decryption) for each of the data set was run thrice and the average of the three values were taken to plot the graphs given below.

We see in Fig. 7, which is a dataset collected 8 months before the YouTube.com hijack incident and Fig. 8, which is collected 8 months after that YouTube.com hijack incident, that the encryption speeds of SPV is at least twice as faster when compared to SiDR.

In case of encryption, the YouTube.com hijack scenario of Full Data dataset for SiDR was slower than SPV by approximately 20%. This is depicted in Fig. 9. For normal case 1 and normal case 2 datasets the encryption times of Full Data for SiDR was slower than SPV by approximately 30%. This is depicted in Fig. 7 and Fig. 8.

In case of decryption, the YouTube.com hijack scenario of Full Data for SiDR was as fast as SPV by less than 2%. This is depicted in Fig. 9. For normal case 1 and normal case 2, the decryption time of SiDR was close to 2% the time taken by SPV.

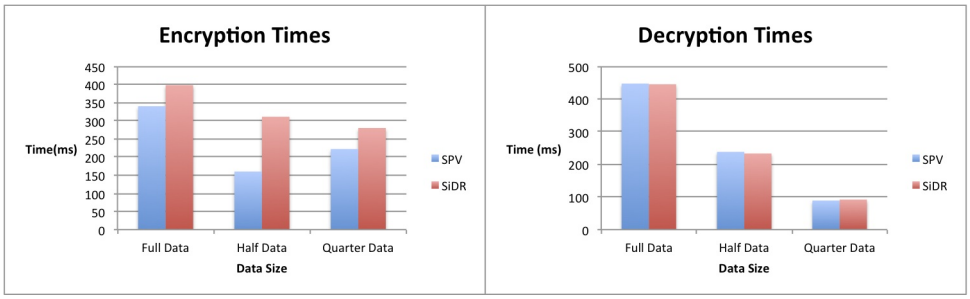

Figure 7: Encryption-decryption times for normal case-1

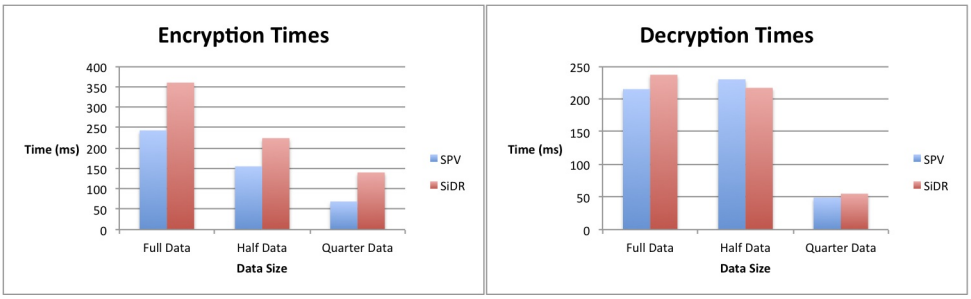

Figure 8: Encryption-decryption times for normal case-2

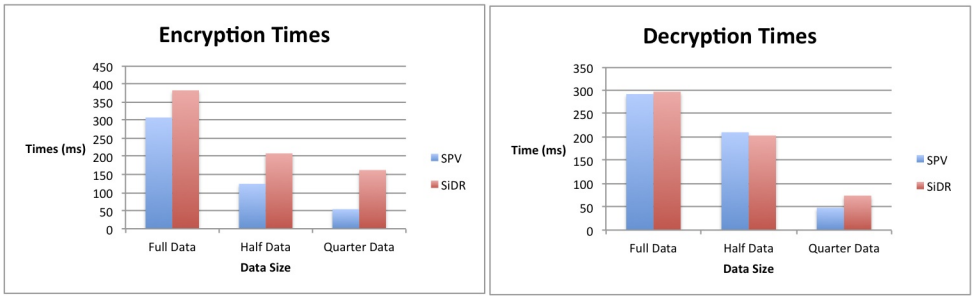

Figure 9: Encryption-Decryption Times for YouTube hijack attack

SiDR key distribution is in built and the communication is based on the attributes itself. Secondly, SiDR follows a hierarchical structure for information hiding and security and hence do not explicitly require digital signature. As explained in the proof section, any entity without a registered set of attributes cannot take part in the communication.

Two major drawbacks of SPV are :

a. Key distribution mechanism is not identified.

b. SPV will require digital certificates for authentication, and hence an processing overhead and key revocation is a issue.

CHAPTER 6

SUMMARY AND FUTURE WORK

In this thesis, we have proposed a novel secure inter domain routing protocol for future Internet in our attempt to solve the vulnerabilities of inter domain routing by leveraging on a novel encryption technique called Attribute Based Encryption. We have proposed the concepts of Dynamic Domain Systems and Dynamic Service Systems as part of the future Internet architecture.

To summarize our work in short words:

- Proposed a new inter domain routing protocol for future Internet by leveraging on novel techniques like Attribute based encryption.
- Logically prove how the proposed architecture is robust against proven attacks.
- Performance and security evaluation of the proposed protocol.

6.1 Future Work - Boot Strapping mechanism

A number of protocols and techniques are available today for enabling bootstrapping. SiDR can benefit from one of these mechanisms tailoring specifically for our purpose. Bootstrapping of SiDR will be the next step in this work. The Session Initiation Protocol (SIP) defined in RFC3261 is a IETF defined signaling protocol for voice and media application sessions. SIP is widely used in the area of Voice-Over-IP applications.

The registration mechanism in SIP can be used as a reference for designing the bootstrapping mechanism of SiDR. SIP has a HTTP like text oriented message format and headers with fields like FROM, TO etc. In SIP the user registers with say his email address and obtains a phone number which can be used to the user through VoIP. The DSS-DSD registration process can also benefit from the Dynamic Host Configuration Protocol where a node requesting a identity (IP in this case) can broadcast its request to a DSD to obtain the attributes and key pairs. However, in addition to this there should also be a off line verification process to ensure the credibility of the entity.

Another approach that can be explored for registration as well as transferring the identity of a DSS from a DSD is the home location register (HLR) and visitor location register (VLR) from the network switching subsystem of a GSM network. When ever a user registered to particular DSD ”visits” another DSD then the DSS can go through a similar authentication center (AUC) based process to transfer the identity from the parent DSD to the current DSD.

The Host Identity Protocol (HIP) specified in RFC 4423 is also another protocol that can be considered to perform the bootstrapping mechanism for SiDR. HIP is a new protocol layer between inter networking and transport layers of the OSI stack. HIP is also a name space for giving a node with a particular identity. HIP name space can also be used as a reference for designing the ”identity” of a DSS, DSD etc.

REFERENCE LIST

[1] ATM Forum Technical Committee. Private Network-Network Interface Specification Version 1.1. Available from. http://www.cisco.com/univercd/cc/td/doc/product/wanbu/bpx8600/pnni_ses/rel11/pnnipg/pintro.htm(2000); accessed 18 August 2011.

[2] Bates, T., Bush, R., Li, T., and Rekhter, Y. DNS-based NLRI origin AS verification in BGP. Available from. http://tools.ietf.org/html/draft-bates-bgp4-nlri-orig-verif-00 (1998); accessed 18 August 2011.

[3] Bethencourt, J., Sahai, A., and Waters, B. Ciphertext-Policy Attribute-Based Cryptography Toolkit. Available from. http://acsc.cs.utexas.edu/cpabe (2006); accessed 18 August 2011.

[4] Bethencourt, J., Sahai, A., and Waters, B. Ciphertext-Policy Attribute-Based Encryption. In Proceedings of the 2007 IEEE Symposium on Security and Privacy (Washington, DC, USA, 2007), SP '07, IEEE Computer Society, pp. 321–334.

[5] Boneh, D. The Decision Diffie-Hellman Problem. In Proceedings of the Third International Symposium on Algorithmic Number Theory (London, UK, 1998), Springer-Verlag, pp. 48–63.

[6] Boneh, D., and Franklin, M. K. Identity-Based Encryption from the Weil Pairing. In Proceedings of the 21st Annual International Cryptology Conference on Advances in Cryptology (London, UK, 2001), CRYPTO '01, Springer-Verlag, pp. 213–229.

[7] Butler, K., Farley, T., McDaniel, P., and Rexford, J. A Survey of BGP Security Issues and Solutions. Proceedings of the IEEE 98, 1 (Jan. 2010), 100 –122.

[8] Caesar, M., and Rexford, J. BGP routing policies in ISP networks. Network, IEEE 19, 6 (Dec. 2005), 5 – 11.

[9] Goodell, G., Aiello, W., Griffin, T., Ioannidis, J., McDaniel, P., and Rubin, A. Working Around BGP: An Incremental Approach to Improving Security and Accuracy of Interdomain Routing. In In Proc. NDSS (2003).

[10] Hu, Y. C., Perrig, A., and Sirbu, M. SPV: Secure Path Vector Routing for Securing BGP. In Proceedings of the 2004 Conference on Applications, Technologies, Architectures, and Protocols for Computer Communications (New York, NY, USA, 2004), SIGCOMM '04, ACM, pp. 179–192.

[11] Huang, D., Ata, S., and Medhi, D. Establishing Secure Virtual Trust Routing and Provisioning Domains for Future Internet. In GLOBECOM 2010, 2010 IEEE Global Telecommunications Conference (Dec. 2010), pp. 1 –6.

[12] Huang, D., Cao, Q., Sinha, A., Schniederjans, M., Beard, C., Harn, L., and Medhi, D. New architecture for intra-domain network security issues. Commun. ACM 49 (Nov. 2006), 64–72.

[13] Huston, G., Rossi, M., and Armitage, G. Securing BGP - A Literature Survey. IEEE Communications Surveys and Tutorials PP, 99 (May 2010), 1–24.

[14] Kent, S., Lynn, C., and Seo, K. Secure Border Gateway Protocol (S-BGP). Selected Areas in Communications, IEEE Journal on 18, 4 (Apr. 2000), 582 –592.

[15] Medhi, D., and Huang, D. Secure and Resilient Routing: Building Blocks for Resilient Network Architectures. In Information Assurance: Dependability and Security in Networked Systems (2008), Elsevier, pp. 417–457. Y. Qian, D. Tipper, P. Krishnamurthy, and J. Joshi (Eds.).

[16] Medhi, D., and Ramasamy, K. Network Routing: Algorithms, Protocols, and Architectures. Morgan Kaufmann Publishers Inc., San Francisco, CA, USA, 2007.

[17] National Defense Magazine. China Internet Hijacking May Have Been Smokescreen for Targeted Attack. Available from. http://www.nationaldefensemagazine.org/blog/Lists/Posts/Post.aspx?ID=254 (2010); accessed 18 August 2011.

[18] Reyzin, L., and Reyzin, N. Better than BiBa: Short One-Time Signatures with Fast Signing and Verifying. In Proceedings of the 7th Australian Conference on Information Security and Privacy (London, UK, UK, 2002), ACISP '02, Springer-Verlag, pp. 144–153.

[19] Routing Information Service. YouTube Hijacking - A RIPE NCC RIS case study. Available from. http://www.ripe.net/

internet-coordination/news/industry-developments/youtube-hijacking-a-ripe-ncc-ris-case-study (2008); accessed 18 August 2011.

[20] The Routing Research Group. The Routing Research Group. Available from. http://irtf.org/rrg(2011); accessed 18 August 2011.

[21] White, R. Securing BGP through secure origin BGP. Internet Protocol Journal 6 (2003).

[22] White, R. Architecture and Deployment Considerations for Secure Origin BGP (soBGP). draft-white-sobgp-architecture-01 (2005).

[23] Zhou, Z., and Huang, D. On efficient ciphertext-policy attribute based encryption and broadcast encryption: extended abstract. In Proceedings of the 17th ACM conference on Computer and communications security (New York, NY, USA, 2010), CCS '10, ACM, pp. 753–755.

VITA

Chockalingam Eswaramurthy was born on March 29, 1986 in Tamil Nadu, India. He was educated in local public schools and graduated from Bharathiya Vidhya Bhavan High School in 2003. After graduating from school, he attended SRM University at Chennai, India, and graduated in May 2007 with a Bachelor degree of Technology in Electronics and Communication Engineering.

After obtaining an undergraduate degree, in May 2007, he worked as Software Engineer at MindTree Ltd from July 2007 - July 2009. After working for two years he joined Masters in Computer Science in University of Missouri–Kansas City at Kansas City, Missouri in August 2009.