Establishing Secure Virtual Trust Routing and Provisioning Domains for Future Internet

Dijiang Huang\textsuperscript{1}, Shingo Ata\textsuperscript{2}, and Deep Medhi\textsuperscript{3}
\textsuperscript{1}Arizona State University, USA
\textsuperscript{2}Osaka City University, Japan
\textsuperscript{3}University of Missouri–Kansas City, USA

Abstract—Secure virtualization is the enabling technique to protect both network providers and user services. Particularly, secure routing in the virtualized service domains is one of the key research areas that have not been explored in literature. In this paper, we present a new secure routing framework to address both network-centric and user-centric networking service models for the future Internet. We aim to provide a flexible network routing framework that has the capability to route traffic with different service requirements and constraints. In other words, it could be highly desirable that two types of network traffic should be isolated either physically or logically and trustworthy services should be avoided to share the bandwidth with normal traffic that may be prone to security attacks. To achieve this capability, we present how to establish a virtual trust routing framework to handle both network-centric routing and user-centric routing simultaneously by using attribute-based cryptography that can provide information-level protection for virtual routing domain isolation. Our performance evaluation on prioritized services through virtual routing domains and cryptography performance analysis demonstrates the viability of the proposed solution.

Index Terms—Secure routing, virtualization, attribute based cryptography.

I. INTRODUCTION

As growth of the Internet infrastructure spreads worldwide, the current Internet has many problems regarding trust communication. For example, there is no fundamental protection mechanism against traffic from untrusted nodes such as malicious traffic, spams, attacks, and scans. Also, end users always have to worry about a risk for drain on information to untrusted parties. These facts make the general public think that the Internet is unsafe. Thus, trustworthiness is a fundamental research issue to be solved for the future Internet.

One of the major pitfalls of current Internet trustworthiness is that the routing infrastructure has limited built-in capabilities to address trustworthiness in both the Internet control plane and the data plane. Current Internet routing is designed to maintain a single packet forwarding table for information flows for all sources and destinations. This all-depends-on-one routing nature has two major inherited drawbacks to respond to attacks.

The first drawback is that the current paradigm makes the network filtering function complicated and prone to errors. For example, to protect routing information at the control plane, IPsec tunnels between routers can be set up to communicate trusted routing information among routers, i.e., a single routing table is established for all-pair traffic. In other words, there is no way to isolate the routing information for trusted data traffic from others. Of course, in the current Internet technology, data traffic from/to an untrusted IP prefix can be blocked by using packet filters configured in routers, to differentiate traffic from various sources and destinations, in the data plane. However, these filters are local functions, i.e., drop/forward packets can be performed only based on the local rules at routers without global traffic engineering capabilities. They can be deployed before and/or after the routing function in the router, which may be very complicated and unable to provide prioritized traffic management at the network level. This nature makes it difficult to provide protection for critical services when the network is under stress.

The second drawback of the current Internet routing is that it is incapable of protecting user traffic for new user-driven service models. Current Internet networking services are network-centric, in which network routing treats packets equally without considering their content. However, in future networks, networking functions, including routing, need to be designed as user-centric in such a way that users have the ability to manage and/or control their packets according to their service requirements. The current cloud computing based services are good examples to demonstrate this trend. Users can request network resources to build their own service domains with fully controlled networking functions – ideally, a user-centric routing paradigm is preferable for this purpose. This is definitely true if we consider the trustworthiness in the function of network routing because trustworthiness is a typical user-oriented metric, i.e., users may require different levels of trustworthiness though traffic flows have the same source and destination nodes. Thus, both user-centric network routing and network-centric routing would need to co-exist in the future Internet.

To address the above described drawbacks, major research challenges are 1) how to construct a trustworthy routing framework at the control plane and 2) how to effectively address both user-centric routing and network-centric routing in order to satisfy different end-users’ service level agreements in the data plane. To address this challenge, a trustworthy routing framework is needed. For example, network routing is planned to have the capability to route traffic with different service requirements and constraints. Trustable services should be avoided to share bandwidth with normal traffic that may be prone to security attacks. Secondly, we consider the mechanism to address security requirements for both network-centric
routing and user-centric routing simultaneously. The traditional approach is to use overlay (or peer-to-peer) networks to satisfy the users’ requirements. However, this approach has three main drawbacks: (i) The failure (or attacks) at the network layer usually cause significant impact at the overlay networks, (ii) The overlay networks usually have a good chance to share the same link due to the shortest path routing at the network layer due to shared risk link groups, and (iii) The trustworthiness of peers is not secured, i.e., there is no way to validate whether all peers in the overlay networks are trustworthy or not. Thus, an attack on the underlying network usually will impact more than one overlay network. In addition, different network service domains may have different trustworthy requirements; thus, some form of traffic regulation may be warranted based on the level of trustworthiness.

This paper positions the current research status and proposes a new future Internet routing infrastructure. An important fundamental question we address is: can we build an integrated routing and trustworthy framework at the network layer level for the future Internet to satisfy both network-centric and user-centric routing requirements? This means that we are interested in a built-in robust approach to trustworthiness at the network layer that is integrated with routing, rather than trustworthiness being ad hoc or an afterthought. Toward this end, we present VTRouPD (Virtual Trust Routing and Provisioning Domain) and µVTRouPD, where the former takes the network-centric view while the latter takes the user-centric view in our overall approach. To this end, we propose a basic notion in future Internet routing: “To architect in a way that virtualizes the network so that different services are clustered into different virtual, adaptive partitions for different services according to their trustworthy requirements”. In considering this notion, it is important to note that a service offering can span the entire spectrum from complete sharing to physically dedicated partitioning. Moreover, different services may be partially overlapped or independent. Furthermore, even without a shared environment, prioritization is also possible, for example, in packet scheduling for different service classes with multiple trust levels at a router.

The rest of the paper is arranged as follows: In Section II, we presented the distinctions between our approach and previous virtualization solutions. In Section III, we present the system and models for the virtual trust routing. In Section IV, we describe the details of each component of the proposed VTRouPD framework. We present a proof-of-the-concept evaluation in Section V. Finally, in Section VI, we conclude our work and point out our future research directions.

II. COMPARISON TO EXISTING VIRTUAL NETWORKING MANAGEMENT APPROACHES

Several recent researches have shown that the research of network management in virtualized networking environments is very active. In [1], the authors presented a programmable hardware platform to construct virtual data planes, which focuses on hardware implementation. In [2], the authors presented VROOM (virtual ROUTers On the Move), which is a new network-management primitive that avoids unnecessary changes to the logical topology by allowing (virtual) routers to freely move from one physical node to another. The research presented in [3] focuses on the accountability in the virtualized hosting environments.

Our presented approach is different from previous approaches in that we focus on building multiple virtualized routing domains through a two-level virtualization approach: (i) using logical virtual routers to partition the physical networking environment into multiple virtual private networks, (ii) using cryptographic methods to further partition a logically virtual network into multiple flow-level virtual routing environments. Our approach provides a fine-grained virtualization for user-centric networking services, and can respond to attacks quickly by using cryptographic approaches. In an earlier work, the basic idea of VTRouPD was introduced [4]; however, this did not consider µVTRouPD, and more importantly, the inter-play between the network-centric and the user-centric considerations.

III. SYSTEM AND MODELS

Our thesis is to address the following features in this work: (a) the network needs to operate in a semi-reservation-oriented mode to allow multiple routing domains to be constructed according to the trust levels of services and they can coexist sharing networking resource, (b) trust management needs to be a built-in factor at the network level to handle security policy federation and enforcement, and (c) entry points to the network have the ability to do authorization checks and/or control traffic when necessary, so that higher trust services can have priority (under stress). In the following two sections, we present our system models at the network service level and information flow level, respectively.

A. Virtual Trust Routing and Provisioning Domain

Our goal is to divide the entire routing domain into multiple routing/provisioning sub-domains. We refer to such a sub-domain as a virtual trust routing and provisioning domain (VTRouPD). The framework may not need/imply the division of the administrative domain into VTRouPDs. Every node that belongs to a particular VTRouPD will have complete
routing information of its own VTRouPD, but not others. Typically, from a systems perspective, traffic management and network resource management components are necessary for monitoring and managing a network. For a trustable environment, there are three additional components involved as shown in Fig. 1: Trust Management Service (TMS), and VTRouPD Domain Manager, and Resource and Application Manager (RAM).

In each VTRouPD, one or multiple Router Instances (RIs) are used for every Routing Service Node (RSN). A Node Manager (NM) is responsible for managing the RIs’ loading and unloading in the RSN. The RAM is the resource manager directed by the VTRouPD manager and TMS to construct VTRouPDs. The VTRouPD manager plays the key role in the new routing framework. TMS is the Trust Authority (TA) for the system. It handles the cryptographic key and parameters distribution and revocation. It also provides identity search and federation services for RSNs belonging to multiple administrative domains, and policy checking and enforcement functions to provide a unified trust management system.

B. Fine-grained Routing Domain Isolation

Here, we present a new, secure, extended node/link update (ENLU) framework by extending a link state routing framework through a secure group communication approach for enabling network virtualization. This scheme allows dissemination of ENLU messages to be encoded in such a way that only nodes with the proper key can take advantage of the encoded information for trustable or prioritized services. We invoke a many-to-many group communication keying scheme presented in [5] to virtualize network resources to support multiple service domains.

Our approach considers two preventive cryptographic countermeasures: confidentiality and authentication. These two countermeasures can provide protection at either the packet level (PL) or the information level (IL), shown in Fig. 2. If we assume a routing packet to be a bus filled with a group of passengers, PL and IL represent the cryptographic countermeasures being provided for the bus and each individual passenger, respectively.

To deploy the information level confidentiality (ILC), routing information (i.e., metric) is categorized by multiple groups. By carefully assigning group keys to nodes, we can partition network resources into multiple routing domains. For example, consider a node with several outgoing links; it can encrypt routing metrics (RMs) for some links using one key and encrypt RMs for other links using another key. Thus, only nodes that have the correct key can decrypt the routing information. This strategy can also be applied to a single link, i.e., a node can partition the bandwidth of a link into multiple portions and create/encrypt an RM for each portion. This approach has several benefits:

- It prevents outsiders’ sniffing attacks (we assume that the crypto key length is long enough to prevent brute force attack within a maintenance cycle, i.e., periodic updating window of the crypto keys).
- It mitigates outsiders’ traffic-analysis attacks: Since extended node/link attributes are encrypted and a node may or may not possess the decrypting key, nodes can maintain different network topology information and shortest path tree or other provisioned paths. Thus, the data flow may not follow the same shortest path that can prevent attackers from deriving the correct network topology or traffic allocation pattern.
- An insider has limited information of the network that can mitigate routing analysis and deliberate exposure attacks.

The above advantages are ideal for our encrypted, extended node/link update (ENLU) approach since it allows us to disseminate ENLU messages in a way that is meant only for a subgroup of nodes. In this paper, for simplicity, we demonstrate our approach by initially considering two services, normal services and trustable services, with the important requirement that trustable services encompass normal services as well. This can be accomplished by defining two subgroups for extended node/link state dissemination using the many-to-many secure group communication scheme we have developed. Note that although there are only two subgroups in this case, which are mapped to two categories of services, the formations of subgroups can be changed frequently with respect to the use of different subgroup keys. This means that if a network wants to define multiple trustable service levels dynamically, our approach allows it with the added advantage that a node can be in different prioritized groups and yet, it cannot become an undesirable node (that is to move to a higher prioritized service class).

IV. ESTABLISH VIRTUAL TRUST ROUTING AND PROVISIONING DOMAINS

We now present the enabling techniques to establish VTRouPDs (virtual trust routing and provisioning domains) that uses a systematic approach to build VTRouPDs. We focus our description in the following areas: (a) the establishment of two levels of VTRouPDs, (b) cryptography-based solution to create fine-grained information-flow level VTRouPDs, and (c) the trust management in VTRouPDs.

A. The Establishment of VTRouPDs

The VTRouPDs architecture is presented in Fig. 1. To establish VTRouPDs, we require network routers to be programmable, i.e., we can create multiple virtual routers (VR) on the same physical router and each VR is responsible for a particular VTRouPD. We present two levels of approaches to deploy the VRs. A the first level, we virtualize independent
router virtual images, where each VR has its own protocol stack and independent IP addresses associated with virtualized interfaces. In this way, traffic can be differentiated at the IP layer through routing functions. For example, the routing table in each VR can mark who the next hop virtual router is. This approach, however, faces certain roadblocks. First, the number of VTRouPDs on each router is restricted by the router’s hardware configuration. This restriction usually makes it impractical to support a large number of VRs running on the same router that further restricts the number of supported VTRouPDs. Second, it is difficult to allow inter-VTRouPDs traffic when services provided by two VTRouPDs are highly correlated and may need merging partial traffic from two VTRouPDs. Thus, the approach using the entire routing function virtualization is only appropriate for network-centric virtualization.

To address the restriction of network-centric routing virtualization, we introduce also a fine-grained routing virtualization at the second level that can take care of users’ service level demands. To this end, we present a complementary concept, virtual trust routing and provisioning sub-domain (noted as VTRouPD), is introduced. A VTRouPD may contain multiple VTRouPDs. In comparison to the VTRouPDs, the boundary of VTRouPDs is not established through virtualizing router functions; instead, we consider virtualization of VTRouPDs through a set of techniques: (a) We use cryptographic packet marking techniques to allow each VR to recognize the traffic flows for different VTRouPDs, (b) We invoke efficient secure group communication solutions to isolate traffic flows that belong to different VTRouPDs. This approach provides us a fine-grained traffic management and filtering capability to identify malicious traffic and reduce the impact to other services when the malicious traffic flows are blocked. Moreover, through secure group-based communication, we can further merge or diverge traffic belonging to different VTRouPDs through super- or sub-group communications. (c) We use an efficient security data access control solution that provides trust party verification, traffic access control, and data privacy protection for VTRouPDs. This capability allows us to provide versatile user-centric network routing services with assured data access policy enforcement and privacy protection. The first level virtualization is straightforward. In the following subsection, we focus on our description on the second level virtualization, and the enabling techniques that will be explored to achieve the above described research.

B. Cryptography-based approaches to create fine-grained µVTRouPDs

Here, we focus on providing information flow isolation for multiple µVTRouPDs. Users belonging to the same µVTRouPDs can “see” the data and the network. A router may belong to multiple µVTRouPDs. Thus, an efficient encryption/decryption scheme must be provided. There are two main issues: (a) establishment of secure group-based communication among µVTRouPDs members and group membership maintenance such as when group members join and leave, and (b) security and privacy policy enforcement for accessing networking information and data within a µVTRouPD, and data sharing among multiple µVTRouPDs. We use an attribute-based data access control mechanism to achieve the described group-based communication system.

![Fig. 3. Attribute-based Encryption.](image)

In Fig. 3, we present an illustration using attribute-based encryption (ABE) [6] for data encryption and decryption. In this example, attributes A1 – A4 are arranged as leaf nodes of the attribute tree, where each attribute can have multiple secret components for different users. We must note that users can share an attribute; however, the corresponding private key components for that attribute are different, and are represented by different colors.

![Fig. 4. An example of ABE for secure group communication.](image)

To present how to use the ABE scheme in secure group communication, we present a simple example consisting of 8 group members in Fig. 4, where each group member (i.e., a router) is associated with a unique binary ID: \( b_0b_1 \ldots b_{n-2}b_{n-1} \), where \( n = \log_2 N \). The cryptography construction is based...
on our recent work [9]. We can use a logic literal, called bit-assignment, $B_i$ and $\overline{B_i}$ to indicate the binary value at position $i$ in an ID. $B_i$ indicates the $i$'th bit of an ID is 1; $\overline{B_i}$ indicates the $i$'th bit of an ID is 0. For a group with $N$ group members, the length of an ID is $n = \log N$ and the total number of bit-assignments is $2n$; that is, two binary values are mapped to one bit position (one for value 0 and one for value 1). We call the set of all possible bit-assignments to be Universe $U$ that contains $2n$ bit-assignments. A group member $u$ is uniquely identified by the set of bit-assignments $S_u$ associated with $u$’s ID. Also, multiple group members may have a common subset of bit-assignments. For example, in Fig. 4, a GM $u_1$’s ID is 000 and a GM $u_2$’s ID is 001, $S_{u_1} = \{\overline{B_0}, \overline{B_1}, B_2\}$ and $S_{u_2} = \{B_0, \overline{B_1}, B_2\}$ and $S_{u_1} \cap S_{u_2} = \{\overline{B_0}, B_1\}$. In a VTRouPD, the group member’s ID (i.e., the router’s ID) can be derived from a hash operation on his unique identifier such as its IP address. Each bit in the ID can be mapped to a predefined attribute (can be a random number), and the user can derive corresponding private key components that mapped to each attribute from a trusted authority.

To form an arbitrary communication group (i.e., $\mu$VTRouPD), suppose a subgroup with $L$ members, a group member can use the Boolean membership functions $M(B_0, B_1, \ldots, B_{n-2}, B_{n-1})$, which is in the form of Sum-of-Product Expression (SOPE), can determine the membership of the subgroup. That is, only if group member $u$ belongs to the subgroup, $M(ID_u) = 1$. Formally, the following properties of membership functions hold:

$$M(b_0^u, b_1^u, \ldots, b_{n-2}^u, b_{n-1}^u) = \begin{cases} 0 & \text{iff } u \in G \setminus L, \\ 1 & \text{iff } u \in L. \end{cases}$$

For example, if the subgroup $L = \{000, 001, 011, 111\}$, then $M = \overline{B_0} \overline{B_1} B_2 + \overline{B_0} B_1 B_2 + B_0 B_1 B_2 + B_0 B_1 B_2$. Using this approach, we can freely construct a super group or subgroups without the key agreement phase, which significantly reduces communication delay. Moreover, this solution achieves the optimal solution that both the communication overhead and storage overhead are $O(\log N)$ in comparison to existing group communication keying schemes.

C. Trust Management in VTRouPDs

Next, consider trust management in VTRouPDs. We first address how to negotiate trust when the virtual routing spans multiple administrative domains, and then we describe the monitoring and attack response system of a VTRouPD.

1) Trust Management among Multiple Administrative Domains: Usually, the trust management is independently managed in different network service administrative domains. Thus, different administrative domains can have different compositions of VTRouPDs. To federate the trust management among VTRouPDs created by different administrative domains, we need to construct a trust negotiation system to address the incurred inconsistency and incompatibility issues.

Another issue due to multiple administrative domains is that a $\mu$VTRouPD can belong to multiple VTRouPDs with different trust levels. Before sending data across multiple VTRouPDs, the system needs to check whether the trust level of the destination VTRouPD has sufficient trust level. However, the trust level is not an absolute value, but a relative (human dependent) value. For example, when two clients communicate with the same server through two different $\mu$VTRouPDs, and their trust levels for the server in their $\mu$VTRouPDs may be different. The node is required to send the data through an appropriate VTRouPD according to its trust level that needs to be satisfied.

The trust level of a $\mu$VTRouPD is also highly related to the privacy requirements, i.e., what types of private information should be contained within a $\mu$VTRouPD or shared among multiple $\mu$VTRouPDs? To regulate the trust management among multiple $\mu$VTRouPDs, we can build the following two levels of mappings:

- Mapping between the privacy sensitivity of the $\mu$VTRouPD information and corresponding trust levels.
- Mapping trust levels among multiple administrative domains.

Another trust management issue is how to initiate trust. To address the trust initialization issue, a reputation based approach can be used. As shown in Fig. 1, the trust management service (TMS) can collect feedback from the system to rank the trust of a router, $\mu$VTRouPD, VTRouPD, and the entire domain of an Internet service provider. Then, TMS can calculate the trust ranking, and provide a recommended trust level for the corresponding party as the initial trust level. The trust level can be measured using the following example metrics:

- Percentage of good traffic transited;
- Reliability of the routing system;
- Trust levels of ingress and egress neighboring domains.

V. PERFORMANCE EVALUATIONS

In this section, we first present a prototyping evaluation when constructing two prioritized network routing domains based on our proposed solution. Then we present the cryptography performance evaluation.

A. Evaluations of Prioritized VTRouPDs

An important question is: can we quantify the benefit in a network that trustable services get allocated prioritized provisioning in a network virtualization framework based on secure encryption? To be able to quantify such a benefit, we have conducted a preliminary simulation.

In our simulation model, we have incorporated protected and dynamic network virtualization by allowing for different service classes, such as a trustable service class over the normal service class. In our preliminary prototype, we have implemented a rudimentary version of the extended node-link update (ENLU) message passing for different service classes. In our current implementation, virtualization is performed on a per link basis; that is, to simulate the affect, a user can decide which links to be considered for virtualization. If this is not considered for virtualization, then all services share the link equally. For activating network virtualization, attributes values of a link are encoded differently for the prioritized
service on a link basis compared to the normal services; this is done so that ENLU messages are recorded by nodes as appropriate for different services in computing routes and service provisioning.

VI. DISCUSSION AND FUTURE WORK

In this work, we present a routing perspective for a secure routing network architecture in which services with differences in trustworthiness, guarantees and priorities can co-exist in a virtualized environment. More importantly, we present a general framework for secure and resilient routing that can be conducive to providing secure traffic engineering in the future Internet. Our approach is forward thinking in that instead of starting with what we require or assume in the network architecture, we start with the need for the service requirement for different levels of trustworthiness in a prioritized environment and work backward to identify what are the different components desirable in the network architecture to support this service paradigm. Implicit in our approach is the basic understanding that we do not necessarily assume that the components are identified to be efficient nor do we claim that all components or solutions have been identified; at times, we expect that some problems identified will remain open, research problems. Thus, an important goal of this paper is to address the fundamental issues in order to arrive at a better understanding of this entire framework.

In future work, we will implement our solution through an education/research platform, such as using NetFPGA [10], and deploy our approach in our GpENI testbed environment [11].

ACKNOWLEDGEMENT

The presented work is supported by US NSF grants CNS-1029562 and CNS-1029546, and Japan NICT grant program “Early-concept Grants for Exploratory Research on New-generation Network”.

REFERENCES