Computer Networks 63 (2014) 128–146

Contents lists available at ScienceDirect

Computer Networks

journal homepage: www.elsevier.com/locate/comnet

# SeRViTR: A framework, implementation, and a testbed for a trustworthy future Internet

Shingo Ata [a], Dijiang Huang [b], Xuan Liu [c], Akira Wada [a], Tianyi Xing [a], Parikshit Juluri [c], Chun-Jen Chung [b], Yasuhiro Sato [d], Deep Medhi [c,e,*]

[a] Graduate School of Engineering, Osaka City University, Osaka, Japan
[b] School of Computing, Informatics and Decision Systems Engineering, Arizona State University, Tempe, AZ, USA
[c] Department of Computer Science and Electrical Engineering, University of Missouri–Kansas City, Kansas City, MO, USA
[d] Faculty of Maritime Safety Technology, Japan Coast Guard Academy, Kure, Japan
[e] Department of Computer Science and Engineering, Indian Institute of Technology–Guwahati, Guwahati, India

ARTICLE INFO

*Article history:*
Received 11 December 2012
Received in revised form 21 November 2013
Accepted 26 December 2013
Available online 3 January 2014

*Keywords:*
Future internet
Internet trustworthiness
Architecture
Prototype
Geo-distributed networks
Network virtualization

ABSTRACT

A flexible, scalable, and robust framework that enables fine-grained flow control under fixed or dynamic policies while addressing trustworthiness as a built-in network level functionality is a desirable goal of the future Internet. Furthermore, the level of trustworthiness may possibly be different from one network to another. It is also desirable to provide user-centric or service-centric routing capabilities to achieve service-oriented traffic controls as well as trust and policy management for security. Addressing these aspects, we present the SeRViTR (Secure and Resilient Virtual Trust Routing) framework. In particular, we discuss the goal and scope of SeRViTR, its implementation details, and a testbed that enables us to demonstrate SeRViTR. We have designed protocols and mechanisms for policy and trust management for SeRViTR and show a validation on the functional implementation of several SeRViTR components to illustrate virtual domains and trust level changes between virtual domains that are achieved under SeRViTR protocols. Going from implementation to testbed, we demonstrate SeRViTR in a virtual network provisioning infrastructure called the Geo-distributed Programmable Layer-2 Networking Environment (G-PLaNE) that connects three institutions spanning the US and Japan.

## 1. Introduction

An important factor that has led to the success of the current Internet is its flexible routing functionality. However, with the rapid growth of the Internet, many issues have risen. One area of interest is trustworthiness, especially at the architectural level. For instance, the current Internet has a limited capability on *trustworthiness* at the network layer level. For example, a secure tunnel (e.g., IPSec [29,30]) at the network layer can be established to exchange information, or access control lists that are used for filtering traffic from unreliable networks by adding network prefixes to their blacklist. An approach such as IPSec is a point-to-point approach, rather than being a network-wide holistic architectural solution. From a routing standpoint, the current Internet provides a simple and network-centric packet forwarding function by only referring to the destination address of the packet where packets are forwarded in the shortest-path manner. However, in the future Internet, it is strongly desirable to have user- or service-centric routing capabilities to achieve service-oriented traffic controls. Additionally, in the future Internet,

[*] Corresponding author at: University of Missouri–Kansas City, Kansas City, MO, USA. Tel.: +1 816 235 2006.

*E-mail addresses:* ata@info.eng.osaka-cu.ac.jp (S. Ata), dijiang.huang@asu.edu (D. Huang), Xuan.Liu@umkc.edu (X. Liu), wada@n.info.eng.osaka-cu.ac.jp (A. Wada), tianyi.xing@asu.edu (T. Xing), pjuluri@mail.umkc.edu (P. Juluri), cchung20@asu.edu (C.-J. Chung), sato@jcga.ac.jp (Y. Sato), dmedhi@umkc.edu (D. Medhi).

1389-1286/$ - see front matter © 2014 Elsevier B.V. All rights reserved.
http://dx.doi.org/10.1016/j.bjp.2013.12.028

to handle various network services' flexibilities and dynamics, routing will be required to be more flexible and have fine-grained flow controls based on a policy while addressing trustworthiness.

Current routing policies provide a functionality on limiting traffic to control what may be allowed. Border Gateway Protocol (BGP) made policy decisions at the AS level so that the AS has the control on redistributing routing information. Another protocol called Inter-Domain Routing Protocol (IDRP) [32] supports access restriction through policies to deny particular traffic transitions. Both BGP and IDRP use path-vector routing, while Inter-Domain Policy Routing (IDPR) [44,43] uses link-state routing to distribute routing policies over managed domains. Here, the managed domains refer to *any collection of contiguous networks* [34] including gateways, links, and hosts whose intra-domain routing manner and service restrictions are controlled by a single administrator. IDPR aims to enforce policies to direct traffic under the users' service requirements, such as bandwidth, acceptable latency, and the paths to avoid. Although those routing policies can provide network resources respecting users' requirements or restrict traffic to some certain path, a more standard and rigorous access control framework at the edges of a routing domain is needed to ensure that the traffic could be trusted.

Policy-based management on the routing framework that provides secure routing is a significant plus on realizing trustworthiness in a virtualized network environment. Having security and trust specification policies enforces access control at the domain level to filter out anomaly traffic so that more secure and better services can be guaranteed from the users' perspective. An adaptive policy-based routing management framework is able to select a managed domain with a proper trust level to direct transit traffic by reviewing the historical behavior of the traffic and the users' service requirements. Note that the traffic behavior refers to the impact on the network performance.

Thus, a flexible, scalable, and robust routing framework that enables fine-grained flow control under fixed or dynamic policies while addressing trustworthiness is a desirable goal. Furthermore, the level of trustworthiness may possibly be different from one network to another, which is also important to allow coexistence. To support flexible traffic control according to various service or user requirements, diversification of routing functionality is also desirable. For this, the network should have virtualization and slicing capabilities according to control policies (for example, for trustworthiness) in place, but that may change dynamically. Delivery of critical traffic in a secure manner by using an isolated slice from other traffic and which is controlled independently should be possible. In addition, the integrated routing framework should support both user- or service-centric traffic controls and provide secured communication with differentiated security requirements. These need to also warrant that the network programmability is a desirable functionality.

Considering the above needs, we present the SeRViTR (Secure and Resilient Virtual Trust Routing) approach. This comprehensive paper is built on our earlier conference and workshop papers [27,33,49]. SeRViTR encompasses three aspects: (1) a framework for a future secure Internet that addresses trustworthiness at the network level, (2) a discussion on how this is implemented, and (3) a geo-distributed testbed that connects three universities between the US and Japan where this functionality is being tested. The core framework builds on the notion of a *Virtual Trusted Routing and Provisioning Domain* (VTRouPD) concept, at both the network level and the service level. A VTRouPD is constructed by a collection of networking resources including routers and switches based on virtualization techniques. Within one or spanning multiple VTRouPDs, we can further create user-centric virtual routing domains that are denoted as $\mu$VTRouPDs.

The paper is organized as follows. We first describe related works in Section 2. We present the scope and the goal of SeRViTR in Section 3. Our design model of SeRViTR with descriptions on detailed operations of key components is presented in Section 4 and Section 5. We next discuss the geo-distributed programmable Layer-2 network environment for the SeRViTR experiment deployment in Section 6 and Section 7. In Section 8, we will briefly introduce the next phase on improving SeRViTR features. We conclude this paper with future research topics in Section 9.

## 2. Related work

Research on the future Internet has been active for years. There are several projects exploring the future Internet infrastructure to provide a large scale programmable networking testbed. GENI [18,46], Global Environment for Network Innovations, is a program exploring the future global networking infrastructure in the United States, where different types of resource provisioning platforms resides. GENI platforms such as PlanetLab [6], ProtoGENI [7], and OpenFlow Networks [35] have different concentrations in terms of provisioning resources, network architecture, programmable networks, and so on. For example, ProtoGENI has integrated a large group of resources available from the world to provide resources with network programmability and sensing features. All GENI-related projects [19,20,39,42,17,45,36] are summarized in Table 1. In particular, DETERLab [17] is a public Emulab-based cyber security research testbed, which supports traffic generation, attack generation, and data analysis capabilities [41]; whereas, Seattle [20] has an efficient design that can easily make spare nodes join their available resource pool to be further utilized to provide Python based experiments.

In Europe, FIRE [2] program is an initiative on the Future Internet architecture design. OneLab [4] is a GENI-like testbed that supports research on the future Internet, as well as the federation between networking research testbeds, in order to establish the international relationship with the future Internet researches in other countries around the world. It is known that GENI has deployed large-scale OpenFlow Networks in the US, and OFELIA [3,25] is the first large-scale programmable OpenFlow Network research environment in Europe. It supports network virtualization capability, new controller testing and customization. Another related effort is Bonfire [1].