Chapter 27
Autonomic Networking Integrated Model and Approach (ANIMA): Secure Autonomic Network Infrastructure

Toerless Eckert
Huawei, USA

ABSTRACT

This chapter presents the work of the Autonomic Networking Integrated Model and Approach (ANIMA) working group of the Internet Engineering Task Force (IETF). It was formed to standardize protocols and procedures for an ANIMA autonomic network (AN) and first chartered to define the ANIMA secure autonomic network infrastructure (ANI). This chapter describes the technical history and goals leading to this working group. It then describes how the ANIMA approach provides an evolutionary approach to securing and automating networks and to provide a common infrastructure to evolve into future autonomic networks. Finally, this chapter compares this approach to adjacent standards technologies and discusses interesting next steps.

INTRODUCTION

Operation, Administration and Maintenance (OAM) as well as service automation within data centers are quickly evolving and driving technology evolution and standards in Software Defined Networks (SDN) and Network Function Virtualization (NFV). Trying to apply these methods to Internet of Things (IoT), Wide Area Networks (WAN), Metro-Area Networks (MAN) or Customer Premises Networks (Enterprises, IoT and others) introduces a range of unique challenges.

OAM and service automation for the above-mentioned networks consist of a highly fragmented and complex set of technologies and practices. One important area is the remotely managed, secured, and automated initial setup of network devices, which is called Zero Touch Deployment (ZTD). Another area

DOI: 10.4018/978-1-6684-3694-3.ch027

is the absence of a common secure and reliable infrastructure for ongoing network OAM and network services control. Vendor- and device-specific solutions are common. These solutions are often complex to manage by themselves and have problems in some topologies such as a multi-layer subtended network ring structures.

The evolving architectural Internet Engineering Task Force (IETF) standards direction for autonomic networks attempts to address these challenges by enabling networks to be self-manageable and self-operational. Ultimately, any network, autonomic or not, should require only high level, so called Intent based input from the operator into the network infrastructure to instantiate its services and direct its operations.

The Network Management Research Group of the Internet Research Task Force analyzed this problem of autonomic networking and published its findings in Behringer et al. (2015) and Jiang et al. (2015). Even before finishing that work, it became clear that any autonomic network would require a common infrastructure and approach for ZTD, secure autonomic network layer communications, discovery and signaling for OAM and network services, and that these components are well enough understood to warrant standardization.

That work resulted in the formation of a working group in the IETF chartered to define and standardize an Autonomic Networking Infrastructure (ANI). This working group is called Autonomic Networking Integrated Model and Approach (ANIMA). In addition to enabling more and more distributed autonomic functions in networks, the ANI targets to support legacy centralized OAM operations as well as current and future centralized SDN methods using a common approach. This chapter presents an overview of that work.

The ANIMA ANI design is currently (2018) targeted to support the most widely deployed type of networks which are managed by professional operators and can thus support a wide range of services and large number of subscribers. These networks often need to evolve over time, adding and changing services and subscribers, and can have high degree of complexity. These networks include Service Provider Networks, Enterprise or Public Networks, but also Industrial and other OT/IoT networks (Operational Technologies, Internet of Things).

Security is a key focus of the ANI because of the recurrent experience with past protocol designs where security was often only considered as an afterthought, resulting either in the inability to deploy solutions due to missing security features and/or high degrees of complexity through later added security functionality.

The most fundamental problem for security is the management of cryptographic keying material. It is also one of the most complex problems in network management. The ANI can use a single Public Key Infrastructure (PKI) certificate on each node for all ANI functions. The Bootstrap of Remote Secure Key Infrastructures protocol (BRSKI) used by the ANI provides a zero touch solution for this problem. It also introduces a novel credential mechanism, called vouchers, to allow booting devices to authenticate the network they are connecting and therefore to mitigate remote attacks against the volatile unconfigured bootstrapping devices.

The ANI relies on a secure, zero touch built, in-band virtual management network. This so-called Autonomic Control Plane (ACP) is indestructible by operator configuration or SDN applications, including mistakes or intentional changes to connectivity/services/security. The ACP provides secure IPv6 connectivity and service discovery not only for OAM/SDN operations, but also to future intelligent distributed autonomic software, which are called Autonomic Service Agents (ASA) in the ANIMA architecture.