Synaptic: A formal checker for SDN-based security policies
Nicolas Schnepf, Rémi Badonnel, Abdelkader Lahmadi, Stephan Merz

To cite this version:
Nicolas Schnepf, Rémi Badonnel, Abdelkader Lahmadi, Stephan Merz. Synaptic: A formal checker for SDN-based security policies. NOMS 2018 - IEEE/IFIP Network Operations and Management Symposium, Apr 2018, Taipei, Taiwan. IEEE, 2018, <10.1109/NOMS.2018.8406122>. <hal-01892397>

HAL Id: hal-01892397
https://hal.archives-ouvertes.fr/hal-01892397
Submitted on 7 Dec 2018

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L’archive ouverte pluridisciplinaire HAL, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d’enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.
Synaptic: a Formal Checker for SDN-based Security Policies

Nicolas Schnepf, Rémi Badonnel, Abdelkader Lahmadi, and Stephan Merz
Université de Lorraine, CNRS, Inria, LORIA, Nancy, France

Abstract
Software-defined networking offers new opportunities for protecting end users by designing dynamic security policies. In particular, security chains can be built by combining security functions, such as firewalls, intrusion detection systems and services for preventing data leakage. The configuration of these security functions and their associated policies is based on behavioural models of end-user applications when accessing the network. In this demo, we present our tool Synaptic, a SDN-based framework intended for the formal verification of security policies as well as for automatically generating such policies based on automata learning methods applied on NetFlow records of end-user applications collected at the device level.

I. Background
The programmability that characterizes SDN [1] simplifies the specification of network policies by decoupling the control and the data planes. Based on this paradigm, it is possible to enforce chains of security functions, such as described in [2] for protecting end users. Such chains are composed of security functions, such as intrusion detection systems, firewalls or data leakage prevention mechanisms, combined in sequence or in parallel. However, due to their complexity and dynamics, these chains of security functions may give rise to misconfigurations in the network. Formal methods provide techniques that can help the validation of security chains before they are deployed. Formal verification of SDN policies is an important topic in the literature [3], [4]. Current approaches focus mostly on the verification of the data plane, and miss aspects related to the control plane. Nevertheless, the Pyretic language [5], part of the Frenetic framework [6], provides an intuitive way for specifying SDN security policies, and verification facilities are provided for the control plane, through its Kinetic extension [7].

II. Synaptic: Generating and Checking Policies
Synaptic combines two functionalities. First, it provides techniques for verifying both the control and data planes related to security chains, as described in [8]. These chains correspond to security policies combining security functions using software-defined networking. Second, it includes a component for profiling applications based on logs of their behavior, and for configuring SDN security policies from the inferred profiles. We developed the prototype using Python 2.7, as an extension of Pyretic and Kinetic. The interactions among

While the checker accepts arbitrary (such as hand-written) security policies expressed in Pyretic, we also support their automatic generation based on automata learning [12]. Synaptic includes a component for learning a Markovian model that captures the networking behavior of an application and for deriving a corresponding security policy in Pyretic. This generation process is divided into four phases depicted in Fig. 2: NetFlow acquisition, NetFlow aggregation, automata learning and rule generation. NetFlow records are collected directly on the end-user device by a dedicated probe, such as Flowoid developed in our research team or from available datasets. Collected NetFlows are transmitted to the aggregation module deployed in the cloud: it will aggregate NetFlows based on the responses of whois requests for the IP addresses and on the ranges of ports contained in the traces. From the aggregated NetFlows, the automaton learning module will infer a Markov chain summarizing the behavior of the application: to do so, we create a state for each pair of netname/port range and we compute the probability of each
outgoing transition. Finally, this automaton is provided to the rule generation module that will generate a Kinetic automaton matching the behavior of the application.

III. THE DEMONSTRATION

In this demo, we will present both the verification and the process learning features of Synaptic. The verification feature will be illustrated with several examples, including the verification of a Kinetic based control automaton or the verification of a stateless firewall. For each of these examples, we will show (1) the policy that input to Synaptic, (2) the properties to be verified, and (3) the verification options offered by Synaptic. We will exhibit correct and erroneous policies, show the corresponding responses of our checker, and provide timing information. For the automata learning feature, we collected traces of different applications. For each of them, we will show how Synaptic can be used for learning a probabilistic model of their networking behavior, and how this can be used to synthesize and then verify a security chain. Through these different examples, we will show how the complexity of NetFlow records influences the automata produced by Synaptic and the response time of the subsequent verification procedure. We will also show how to configure the aggregation module in order to reduce this complexity as much as possible. Finally, we will illustrate how automata can be stored in external files in order to be processed by other services: an example of such an automaton appears in Fig. 3.

Figure 2. Generation and verification of SDN-based security policies based on application profiling.

Figure 3. Automaton describing the behavior of the Dropbox application.

REFERENCES