Offloading personal security applications to a secure and trusted network node

Offloading personal security applications to a secure and trusted network node

R. Bonafiglia[§], F. Ciaccia[¶], A. Lioy[§], M. Nemirovsky[‡‡], F. Risso[§], T. Su[§]
[§]Politecnico di Torino, Dip. Automatica e Informatica, Italy
[¶]Barcelona Supercomputing Center (BSC), Spain
[‡‡]ICREA Researcher Professor at Barcelona Supercomputing Center (BSC), Spain

***Abstract*—The current device-centric protection model against security threats has serious limitations from the final user perspective, among the other the necessity to keep each device updated with the latest security updates and the necessity to replicate all the security polices across all devices. In our model, the protection is decoupled from the users terminals and it is provided through a Trusted Virtual Domain (TVD) instantiated in future edge routers. Each TVD provides unified and homogeneous security for a single user, irrespective of the terminal employed. This paper shows a first prototype implementing this concept through a network element, called Network Edge Device, capable of running the proposed virtualized architecture and making extensive use of SDN technologies, with the aim at providing a uniform security level for the final user.**

I. Introduction

Today's classical approach to the security of personal devices requires the installation of security software directly on the devices that need to be protected. With a growing number of user terminals (laptops, smartphones, smart TVs, and more), keeping all those devices protected has become a challenge; achieving a uniform level of security across all of them would be even harder. In fact, each device needs to be configured with the proper security policies, while security patches (e.g. related to the operating system and/or the installed software) needs to be readily applied. However, this may not always be possible, as some devices (e.g. smart TVs) may not support the desired set of security properties, or security patches may not be promptly released by the software manufacturer[1]. The above problems can be mitigated by processing all the network traffic in a security device operating close to the user, possibly integrated in an home gateway or an edge router. In a nutshell, we propose to *offload security* to a *personal* Trusted Virtual Domain (TVD) running in an *Network Edge Device* (NED), in charge of executing all the user's security applications on the network traffic, regardless of the personal device in use, thus reaching *uniform network protection*. This paper introduces the main architectural components of the NED, followed by a description of a prototype developed based on the above architecture; finally a demonstration scenario of the prototype is presented.

[1]It is worth mentioning that some versions of mainstream operating systems, such as Android, Apple IOS or Microsoft Windows, are no longer covered by the proper security patches, although their penetration in the market is still far from marginal.

II. Architecture

A. The TVD

The Trusted Virtual Domain is the main component of this architecture: it is a logical container of all the user network security. Each security control processes exclusively the traffic of a single user, thus is called a Personal Security Application (PSA). It runs in an Execution Environment (EE); the EE is a placeholder for the PSA execution which should be adequately separated from other users' environment, guaranteeing traffic isolation. Multiple PSAs for the same user can run in the same EE in cascade. PSAs behaviour is monitored by another component, the Personal Security Controller (PSC) which is also in charge of configuring PSAs at startup time; the PSC runs in a separate EE. The TVD is Trusted as all the components (hardware and software) are being *attested* following the principles of Trusted Computing [1]. In this way is possible to verify that the software running on the NED is not tampered according to some *golden measurements*.

B. The TVD Manager

The TVD Manager (TVDM) is the architecture Orchestration and Management component. Once the user is authenticated in the system, the TVDM deals with the requests to instantiate a new TVD by determining the resources required for its allocation and then commanding the deployment. The TVDM performs an analysis of the required virtualization technology and the management of the network topology (physical and virtual) to support the deployment of the whole user's Service Graph (SG). The SG is the formalism that describes the service requested by the user and it is, in its simplest form, a set of cascaded PSAs active on the user's traffic. The SG is defined as the superposition of two directed graphs in which nodes represent the PSAs and arcs represent the flow of the traffic between two nodes. Arcs can be labelled with a set of packet filtering rules (e.g. OpenFlow Flowmods) that select which traffic has to flow through that arc in that direction. The TVDM is in charge of translating this abstract model into actual flow rules to be pushed in the virtual switches, thus acting as an OpenFlow controller.

C. The PSC Manager

The PSC Manager (PSCM) is the front-end component of the architecture; it includes the NED Authentication system which can be implemented either locally or using an external