XXXIII SIC SALÃO INICIAÇÃO CIENTÍFICA

Evento	Salão UFRGS 2021: SIC - XXXIII SALÃO DE INICIAÇÃO CIENTÍFICA DA UFRGS
Ano	2021
Local	Virtual
Título	Melhorando a Segurança do Plano de Controle de SDNs com Controle de Fluxo de Informação
Autor	IVAN PETER LAMB
Orientador	JOSÉ RODRIGO FURLANETTO DE AZAMBUJA

Autor: Ivan Peter Lamb

Orientador: José Rodrigo Furlanetto de Azambuja

Título: Melhorando a Segurança do Plano de Controle de SDNs com Controle de Fluxo de Informação.

O plano de controle é uma peça fundamental de redes definidas por software (SDNs), sendo necessário garantir um nível aceitável de integridade para que a rede como um todo não seja comprometida. Ataques CAP (Cross App Poisoning) recentemente ganharam espaço de discussão no tópico de segurança, e este trabalho visa enriquecer as soluções para esse problema emergente. O objetivo do trabalho é melhorar o Plano de Controle do projeto PvS (Programable Virtual Switches) para torná-lo resiliente a ataques CAP. A solução deve ser flexivel, podendo ser aplicada em outros controladores SDN com poucas modificações. Partindo dos conceitos fundamentais de uma solução existente (ProvSDN), incluindo grafo de proveniência, “labels” de integridade e controle de fluxo de informação, o projeto extendeu o conceito para ambientes com switches virtuais (PvS), permitindo a infêrencia de fluxos “fora de banda”, aos quais o Plano de Controle não possúi acesso direto. Para testar os resultados, foram propostos dois ataques CAP a uma rede SDN executando sob um controlador ONOS, que devem ser detectados e bloqueados pelo sistema. Esses ataques exploram (1) uma aplicação de encaminhamento reativo, que configura tabelas de switches baseado em “table misses” e (2) uma aplicação de telemetria “in band”, que monitora e reconfigura o tráfego de pacotes na rede em casos de congestionamento de filas. O sistema implementado é capaz de detectar e bloquear os ataques dos casos de teste. O custo computacional adicional desse sistema de segurança é aceitável quando se considera seus benefícios. Atualmente o foco do trabalho é extender o sistema de políticas para oferecer mais controle ao administrador da rede e combater os falsos positivos detectados.