Cross-App Poisoning in Software-Defined Networking

Submitted by awhitesell on Mon, 10/15/2018 - 1:34pm

Title	Cross-App Poisoning in Software-Defined Networking
Publication Type	Conference Paper
Year of Publication	2018
Authors	Benjamin E. Ujcich, University of Illinois at Urbana-Champaign, Samuel Jero, MIT Lincoln Laboratory, Anne Edmundson, Princeton University, Qi Wang, University of Illinois at Urbana-Champaign, Richard Skowyra, MIT Lincoln Laboratory, James Landry, MIT Lincoln Laboratory, Adam Bates, University of Illinois at Urbana-Champaign, William H. Sanders, University of Illinois at Urbana-Champaign, Cristina Nita-Rotaru, Northeastern University, Hamed Okhravi, MIT Lincoln Laboratroy
Conference Name	2018 ACM Conference on Computer and Communications Security
Date Published	October 2018
Publisher	ACM
Conference Location	Toronto, Canada
Keywords	data provenance, Information Flow Control, Monitoring, Fusion, and Response for Cyber Resilience, network operating system, NSA SoS Lablets Materials, Policy-Governed Secure Collaboration, software-defined networking, UIUC
Abstract	Software-defined networking (SDN) continues to grow in popularity because of its programmable and extensible control plane realized through network applications (apps). However, apps introduce significant security challenges that can systemically disrupt network operations, since apps must access or modify data in a shared control plane state. If our understanding of how such data propagate within the control plane is inadequate, apps can co-opt other apps, causing them to poison the control plane's integrity. We present a class of SDN control plane integrity attacks that we call cross-app poisoning (CAP), in which an unprivileged app manipulates the shared control plane state to trick a privileged app into taking actions on its behalf. We demonstrate how role-based access control (RBAC) schemes are insufficient for preventing such attacks because they neither track information flow nor enforce information flow control (IFC). We also present a defense, ProvSDN, that uses data provenance to track information flow and serves as an online reference monitor to prevent CAP attacks. We implement ProvSDN on the ONOS SDN controller and demonstrate that information flow can be tracked with low-latency overheads.
URL	http://publish.illinois.edu/science-of-security-lablet/files/2018/10/Cross-App-Poisoning-in-Software...
Citation Key	node-56327

Attachment	Taxonomy	Kind	Size

Cross-App Poisoning in Software-Defined Networking	data provenance Information Flow Control network operating system software-defined networking Policy-Governed Secure Collaboration Monitoring, Fusion, and Response for Cyber Resilience UIUC UIUC NSA SoS Lablets Materials	PDF document	1.15 MB	Download Preview

data provenance Information Flow Control network operating system software-defined networking UIUC NSA SoS Lablets Materials Policy-Governed Secure Collaboration UIUC Policy-Governed Secure Collaboration UIUC Monitoring, Fusion, and Response for Cyber Resilience