SDN Teleportation: Exploiting the OpenFlow Handshake

Kashyap Thimmaraju
Security in Telecommunications
Technische Universität Berlin
Germany

2nd ONOS Security and Performance Brigade Plenary Workshop
11 April, 2018, LIP6, Paris, France

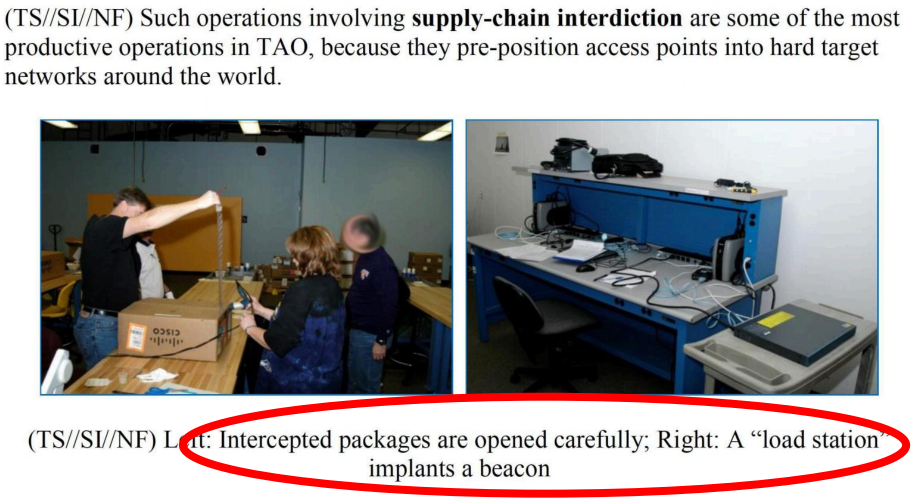
Agenda

- SDN Teleportation
- OpenFlow Handshake Vulnerability CVE-2018-1000155

Inspiration

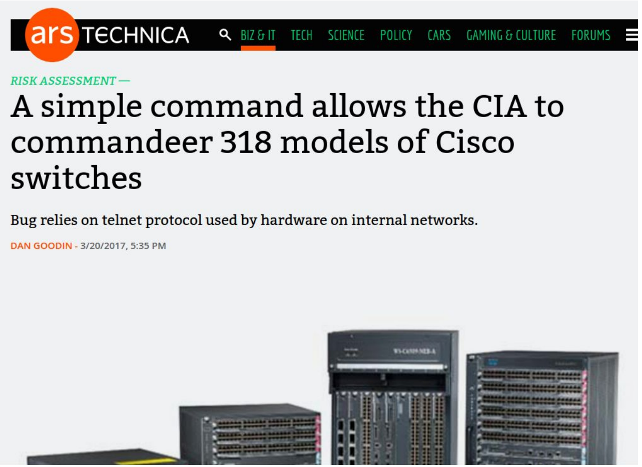
Bundesamt
für Sicherheit in der
Informationstechnik

Backdoors



(TS//SI//NF) Such operations involving **supply-chain interdiction** are some of the most productive operations in TAO, because they pre-position access points into hard target networks around the world.

(TS//SI//NF) Left: Intercepted packages are opened carefully; Right: A "load station" implants a beacon



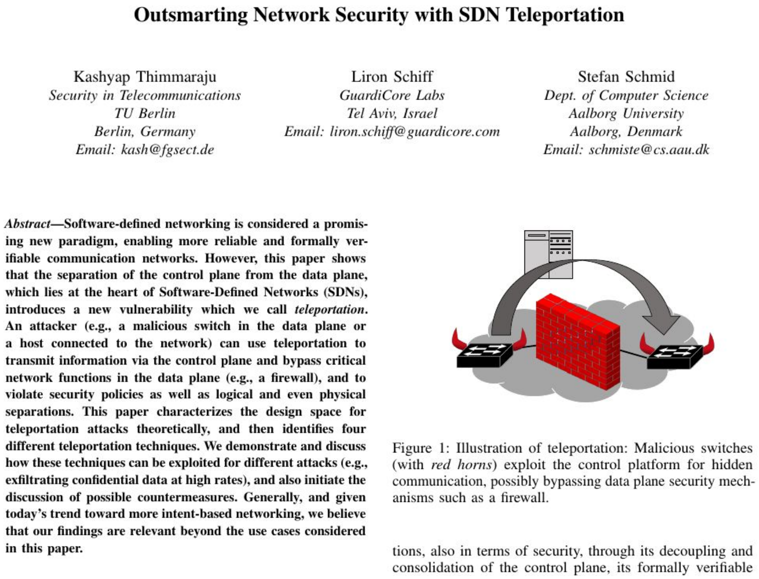
RISK ASSESSMENT —

A simple command allows the CIA to commandeer 318 models of Cisco switches

Bug relies on telnet protocol used by hardware on internal networks.

DAN GOODIN - 3/20/2017, 5:35 PM

SDN Teleportation (EuroSP’17)



Outsmarting Network Security with SDN Teleportation

Kashyap Thimmaraju
Security in Telecommunications
TU Berlin
Berlin, Germany
Email: kash@fgsect.de

Liron Schiff
GuardiCore Labs
Tel Aviv, Israel
Email: liron.schiff@guardicore.com

Stefan Schmid
Dept. of Computer Science
Aalborg University
Aalborg, Denmark
Email: schmiste@cs.aau.dk

***Abstract*—Software-defined networking is considered a promising new paradigm, enabling more reliable and formally verifiable communication networks. However, this paper shows that the separation of the control plane from the data plane, which lies at the heart of Software-Defined Networks (SDNs), introduces a new vulnerability which we call *teleportation*. An attacker (e.g., a malicious switch in the data plane or a host connected to the network) can use teleportation to transmit information via the control plane and bypass critical network functions in the data plane (e.g., a firewall), and to violate security policies as well as logical and even physical separations. This paper characterizes the design space for teleportation attacks theoretically, and then identifies four different teleportation techniques. We demonstrate and discuss how these techniques can be exploited for different attacks (e.g., exfiltrating confidential data at high rates), and also initiate the discussion of possible countermeasures. Generally, and given today’s trend toward more intent-based networking, we believe that our findings are relevant beyond the use cases considered in this paper.**

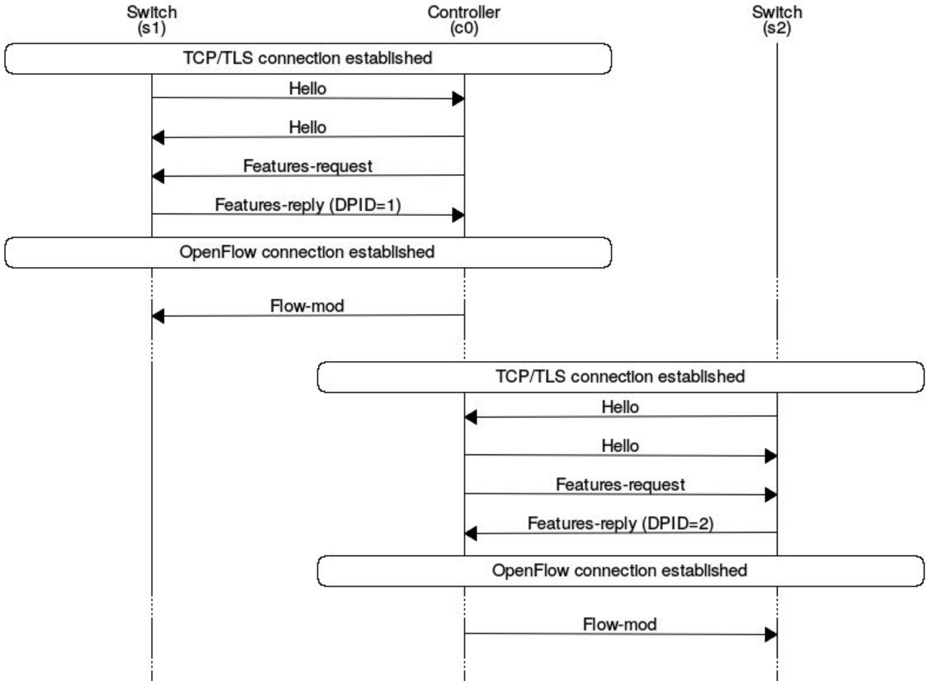
Figure 1: Illustration of teleportation: Malicious switches (with *red horns*) exploit the control platform for hidden communication, possibly bypassing data plane security mechanisms such as a firewall.

tions, also in terms of security, through its decoupling and consolidation of the control plane, its formally verifiable

Switch Identification Teleportation

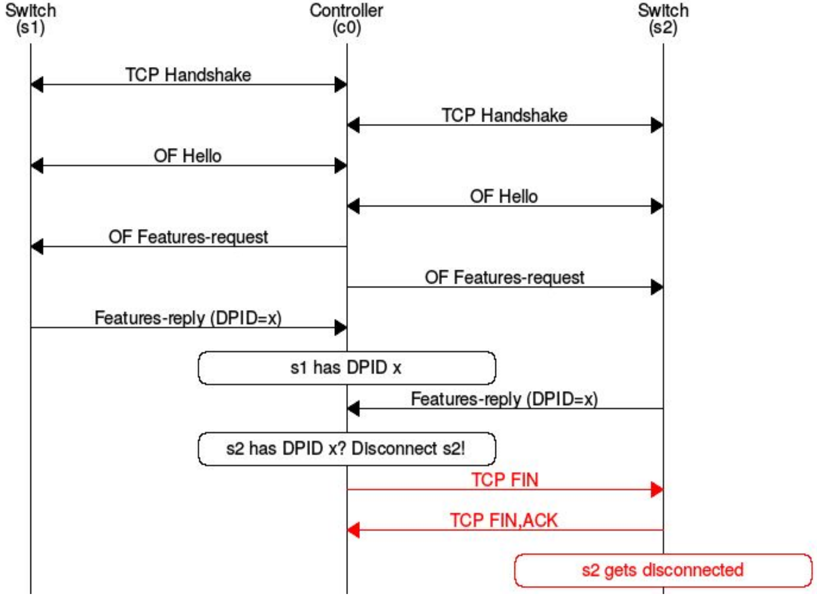
- OpenFlow Handshake
- Switches use the same Data Path Identifier (DPID) to the same controller

OpenFlow Handshake



Switch Identification Teleportation

With ONOS



Switch (s1)

Controller (c0)

Switch (s2)

TCP Handshake

TCP Handshake

OF Hello

OF Hello

OF Features-request

OF Features-request

Features-reply (DPID=x)

s1 has DPID x

Features-reply (DPID=x)

s2 has DPID x? Disconnect s2!

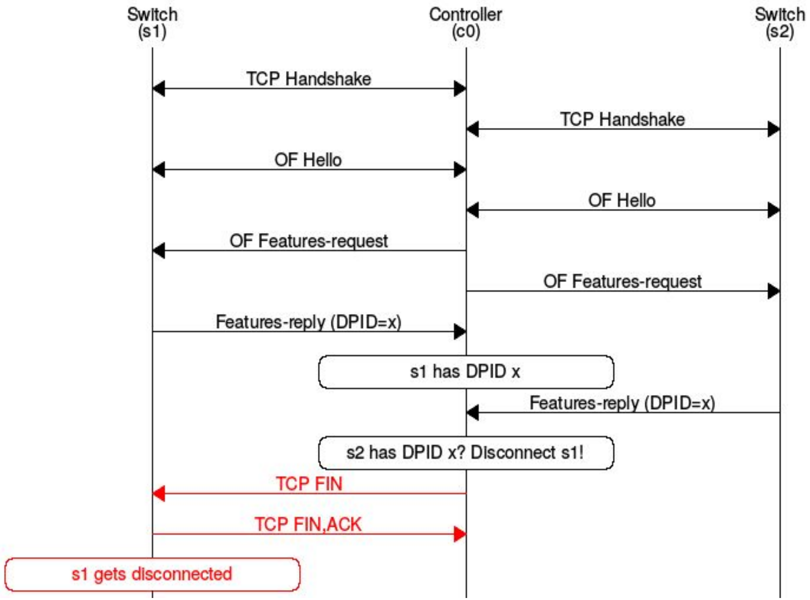
TCP FIN

TCP FIN,ACK

s2 gets disconnected

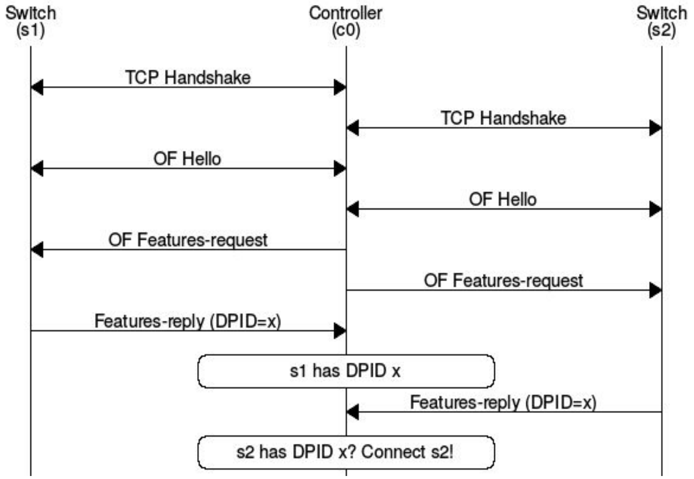
Switch Identification Teleportation

With FloodLight [Dover] and OpenDaylight



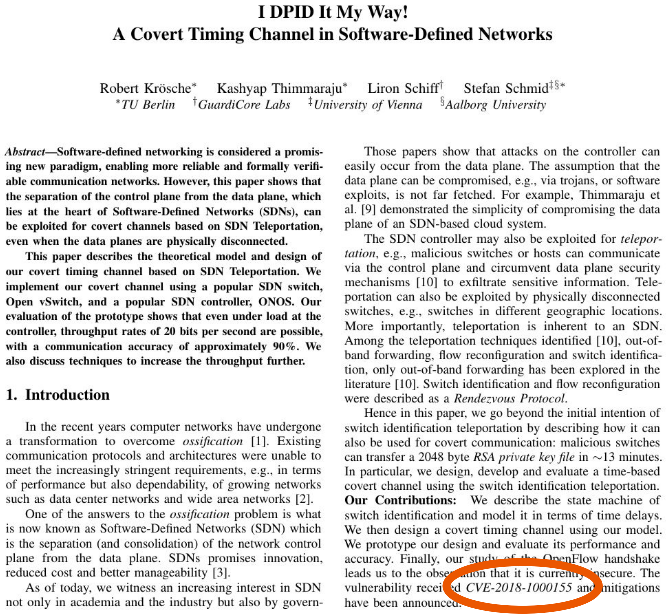
Switch Identification Teleportation

With RYU



SDN Covert Timing Channel (Networking 2018)

- Switch Id Teleportation with ONOS
- Can reach 20bps with ~90% accuracy in our setup
- **CVE-2018-1000155**



I DPID It My Way!
A Covert Timing Channel in Software-Defined Networks

Robert Krösche[*] Kashyap Thimmaraju[*] Liron Schiff[†] Stefan Schmid[‡§*]
[*]*TU Berlin* [†]*GuardiCore Labs* [‡]*University of Vienna* [§]*Aalborg University*

***Abstract*—Software-defined networking is considered a promising new paradigm, enabling more reliable and formally verifiable communication networks. However, this paper shows that the separation of the control plane from the data plane, which lies at the heart of Software-Defined Networks (SDNs), can be exploited for covert channels based on SDN Teleportation, even when the data planes are physically disconnected.**

This paper describes the theoretical model and design of our covert timing channel based on SDN Teleportation. We implement our covert channel using a popular SDN switch, Open vSwitch, and a popular SDN controller, ONOS. Our evaluation of the prototype shows that even under load at the controller, throughput rates of 20 bits per second are possible, with a communication accuracy of approximately 90%. We also discuss techniques to increase the throughput further.

1. Introduction

In the recent years computer networks have undergone a transformation to overcome *ossification* [1]. Existing communication protocols and architectures were unable to meet the increasingly stringent requirements, e.g., in terms of performance but also dependability, of growing networks such as data center networks and wide area networks [2].

One of the answers to the *ossification* problem is what is now known as Software-Defined Networks (SDN) which is the separation (and consolidation) of the network control plane from the data plane. SDNs promises innovation, reduced cost and better manageability [3].

As of today, we witness an increasing interest in SDN not only in academia and the industry but also by govern-

Those papers show that attacks on the controller can easily occur from the data plane. The assumption that the data plane can be compromised, e.g., via trojans, or software exploits, is not far fetched. For example, Thimmaraju et al. [9] demonstrated the simplicity of compromising the data plane of an SDN-based cloud system.

The SDN controller may also be exploited for *teleportation*, e.g., malicious switches or hosts can communicate via the control plane and circumvent data plane security mechanisms [10] to exfiltrate sensitive information. Teleportation can also be exploited by physically disconnected switches, e.g., switches in different geographic locations. More importantly, teleportation is inherent to an SDN. Among the teleportation techniques identified [10], out-of-band forwarding, flow reconfiguration and switch identification, only out-of-band forwarding has been explored in the literature [10]. Switch identification and flow reconfiguration were described as a *Rendezvous Protocol*.

Hence in this paper, we go beyond the initial intention of switch identification teleportation by describing how it can also be used for covert communication: malicious switches can transfer a 2048 byte *RSA private key file* in ∼13 minutes. In particular, we design, develop and evaluate a time-based covert channel using the switch identification teleportation.
Our Contributions: We describe the state machine of switch identification and model it in terms of time delays. We then design a covert timing channel using our model. We prototype our design and evaluate its performance and accuracy. Finally, our study of the OpenFlow handshake leads us to the observation that it is currently insecure. The vulnerability received *CVE-2018-1000155* and mitigations have been announced.

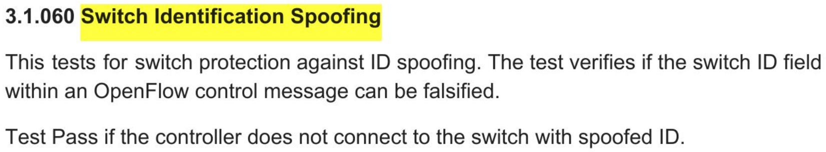
ONOS Security and Performance Analysis: Report No. 1

Stefano Secci, Kamel Attou, Dung Chi Phung,
Sandra Scott-Hayward*, Dylan Smyth°, Suchitra Vemuri#, You Wang#

LIP6, UPMC Sorbonne, Paris, France.
*CSIT, QUB, Belfast, UK.
°Nimbus Centre, CIT, Cork, Ireland.
#Open Networking Foundation, ONF, Menlo Park, USA.

Corresponding author: Stefano Secci (stefano.secci@lip6.fr)

Date: September 19, 2017



3.1.060 Switch Identification Spoofing

This tests for switch protection against ID spoofing. The test verifies if the switch ID field within an OpenFlow control message can be falsified.

Test Pass if the controller does not connect to the switch with spoofed ID.

CVE-2018-1000155: OF Handshake Vuln.

- Lack of authentication
- Lack of authorization
- Denial of service
- Difficult to specify the outcome for a switch ID collision at the controller in OpenFlow
- Public announcement some time in May

CVE-2018-1000155: Proposed Mitigation

- Unique TLS certificates for switches
- White-list of switch DPIDs at controllers [Gray et al.] and the switches’ respective public-key certificate identifier
- A controller mechanism that verifies the DPID announced in the OpenFlow handshake is over the TLS connection with the associated (DPID) certificate

Contact

Kashyap Thimmaraju

Email: kash@sect.tu-berlin.de

Web: www.fgsect.de/~hashkash

Fingerprint: 5FFC 5589 DC38 F6F5 CEF7 79D8 A10E 670F 9520 75CD

References

1. [Gray et al.] N. Gray, T. Zinner, and P. Tran-Gia, “Enhancing sdn security by device fingerprinting,” In Proc. IFIP/IEEE International Symposium on Integrated Network Management (IM), May 2017.
2. [Thimmaraju et al.] K. Thimmaraju, L. Schiff, and S. Schmid, “Outsmarting network security with sdn teleportation,” in Proc. IEEE European Security & Privacy (S&P), 2017.
3. [Krösche et al.] R. Krösche, K. Thimmaraju, L. Schiff, and S. Schmid, “I DPID It My Way! A Covert Timing Channel in Software-Defined Networks ,” to appear in Proc. IFIP Networking, 2018.
4. [Dover] J. M. Dover, “A denial of service attack against the open floodlight sdn controller,” Dover Networks, Tech. Rep., 2013. [Online]. Available: http://dovernetworks.com/wp-content/uploads/ 2013/12/OpenFloodlight-12302013.pdf
5. [Secci et al.] S. Secci, K. Attou, D. C. Phung, S. Scott-Hayward, D. Smyth, S. Vemuri and You Wang, “ONOS Security and Performance Analysis: Report No. 1” ONOS, 2017.