Taking Control of SDN-based Cloud Systems via the Data Plane

Kashyap Thimmaraju
Security in Telecommunications
TU Berlin
Berlin, Germany
kash@sect.tu-berlin.de

Bhargava Shastry
Security in Telecommunications
TU Berlin
Berlin, Germany
bshastry@sect.tu-berlin.de

Tobias Fiebig
Faculty of Technology, Policy and Management
TU Delft
Delft, Netherlands
t.fiebig@tudelft.nl

Felicitas Hetzel
Security in Telecommunications
TU Berlin
Berlin, Germany
file@sect.tu-berlin.de

Jean-Pierre Seifert
Security in Telecommunications
TU Berlin
Berlin, Germany
jpseifert@sect.tu-berlin.de

Anja Feldmann
Internet Network Architectures
TU Berlin
Berlin, Germany
anja@inet.tu-berlin.de

Stefan Schmid∗†
Faculty of Computer Science
University of Vienna
Vienna, Austria
schmieste@univie.ac.at

ABSTRACT
Virtual switches are a crucial component of SDN-based cloud systems, enabling the interconnection of virtual machines in a flexible and “software-defined” manner. This paper raises the alarm on the security implications of virtual switches. In particular, we show that virtual switches not only increase the attack surface of the cloud, but virtual switch vulnerabilities can also lead to attacks of much higher impact compared to traditional switches.

We present a systematic security analysis and identify four design decisions which introduce vulnerabilities. Our findings motivate us to revisit existing threat models for SDN-based cloud setups, and introduce a new attacker model for SDN-based cloud systems using virtual switches.

We demonstrate the practical relevance of our analysis using a case study with Open vSwitch and OpenStack. Employing a fuzzing methodology, we find several exploitable vulnerabilities in Open vSwitch. Using just one vulnerability we were able to create a worm that can compromise hundreds of servers in a matter of minutes.

Our findings are applicable beyond virtual switches: NFV and high-performance fast path implementations face similar issues. This paper also studies various mitigation techniques and discusses how to redesign virtual switches for their integration.

KEYWORDS
Network Isolation; Network Virtualization; Data Plane Security; Packet Parsing; MPLS; Virtual Switches; Open vSwitch; Cloud Security; OpenStack; Attacker Models; ROP; SDN; NFV

1 INTRODUCTION
Modern cloud systems such as OpenStack [1], Microsoft Azure [2] and Google Cloud Platform [3] are designed for programmability, (logically) centralized network control and global visibility. These tenets also lie at the heart of Software-defined Networking (SDN) [4, 5] which enables cloud providers to efficiently utilize their resources [6], manage their multi-tenant networks [7], and reason about orchestration [8].

The data plane of Software-Defined Networks in the cloud are highly virtualized [7]: Virtual switches (running on the servers) are responsible for providing connectivity and isolation among virtual machines [9]. Prominent virtual switches today are: Open vSwitch (OvS) [10], Cisco Nexus 1000V [11], VMware vSwitch [12] and Microsoft VFP [2].

Virtual switches are typically not limited to provide traditional switching but support an increasing number of network and middlebox functionality [2, 13], e.g., routing, firewalling, network address translation and load-balancing. Placing such functionality at the virtualized edge of the network (i.e., the servers) is attractive, as it allows to keep the network fabric simple and as it supports scalability [2, 9].

However, the trend to move functionality from the network fabric to the edge (virtual switch) also comes at the price of increased complexity. For example, the number of protocols that need to be parsed and supported by virtual switches (Open vSwitch and Cisco Nexus 1000v) and OpenFlow [4] have been growing steadily over the last years [14] (see Fig. 1).

The trend towards more complex virtual switches is worrisome as it may increase the attack surface of the virtual switch. For example, implementing network protocol parsers in the virtual switch is non-trivial and error-prone [15, 16]. These observations lead us in this paper to conduct a security study of virtual switches.
Our contributions:

- We present a systematic security analysis of virtual switches. We find that virtual switches not only increase the attack surface of an SDN-based cloud system (compared to their traditional counterparts), but can also have a much larger impact on cloud systems.
- Our analysis reveals four main factors that cause security issues: The co-location of virtual switches with the server’s virtualization layer (in user- and kernel-space); centralized control; complex packet parsing (and processing) of attacker controlled data.
- Our findings motivate us to revisit current threat models. We observe that existing models do not encompass the security issues identified in this paper leading us to introduce a new attacker model for the operation of virtualized data plane components in a Software-defined Network as well as in the context of Network Function Virtualization (NFV): A low-budget attacker can cause significant harm on SDN-based cloud systems.
- We demonstrate the practical feasibility of our attacks on OvS, a popular open-source virtual switch implementation used in SDN-based cloud systems. This case study shows that commonly used virtual switch implementations are not resilient against our attacker model. Indeed, such an attacker can successfully exploit a whole SDN-based cloud setup within minutes.
- We extend our study by surveying high performance fast paths, other virtual switch implementations, and related SDN and NFV technologies. We find that they are also susceptible to the same design issues. Furthermore, we find that software mitigations are commonly not considered during the evaluation of new data plane components.
- We find that software mitigations for the vulnerabilities we exploited could be adopted with a small performance penalty for real-world traffic scenarios. Their use must be evaluated during design and implementation of new SDN and NFV components.

Ethical Considerations: To avoid disrupting the normal operation of businesses, we verified our findings on our own infrastructure. We have disclosed our findings to the OvS team who have integrated the fixes. Ubuntu, Redhat, Debian, Suse, Mirantis, and other stakeholders have applied these fixes in their stable releases. Furthermore, CVE-2016-2074 and CVE-2016-10377 were assigned to the discovered vulnerabilities.

Structure: We provide necessary background information on SDN in the cloud and virtual switches in Section 2. Section 3 introduces and discusses our security analysis of virtual switches and existing threat models. Based on this analysis we propose a new attacker model. Section 4 presents a proof-of-concept case study attack on OvS in OpenStack. We then investigate how our findings on OvS relate to other virtual switches, high performance fast paths and SDN/NFV in Section 5. Subsequently, we discuss possible software mitigations and their performance impact in Section 6, and design countermeasures in Section 7. After discussing related work in Section 8, we conclude in Section 9.

2 BACKGROUND

This section reviews the background necessary to understand the remainder of this paper.

2.1 SDN in the Cloud

Centralized network control and network-wide view are key design goals for state-of-the-art cloud operating systems such as OpenStack [1] and other commercial cloud providers, e.g., Google Cloud Platform [3]. Data plane isolation is typically ensured using separate physical/logical networks (guest, management and external) and tunneling technologies [17] such as VLAN, GRE, VXLAN, MPLS, etc. A cloud network generally comprises of a physical network consisting of physical switches interconnecting virtualized servers and an overlay (virtual) network interconnecting the VMs. The centralized control is attractive as it reduces the operational cost and complexity of managing cloud networks [18]. It also provides flexibility for managing and using cloud services, including VM migration. In addition, the servers in the cloud are connected to external networks (e.g., Internet) via a network node (router). In SDN, OpenFlow [4] is the de facto standard south bound protocol. Via the OpenFlow API, the controller can add, remove, update, and monitor flow tables and their flows.

2.2 Virtual Switches

The network’s data plane(s) can either be distributed across virtualized servers or across physical (hardware) switches. OvS, VMware vSwitch, and Cisco Nexus 1000V are examples of the former and are commonly referred to as virtual switches. Cisco VN-Link [19] and Virtual Ethernet Port Aggregator (VEPA) [20] are examples of the latter.

Virtual switches have the advantage that inter-VM traffic, i.e., traffic between VMs on the same server, does not leave that server. The performance overhead of software-only switching (e.g., OvS) can be alleviated by hardware-offloading features: While traditionally, such features were only available in expensive proprietary networking equipment, they are currently gaining traction. For example, Pettit et al. [21] showed that the performance of OvS and VEPA are comparable when executing on a remote bare-metal server. Indeed, OvS performs better for large transfers at high rates when executing on the same server.
The requirements as well as the operating environment for virtual switches differs significantly from that of traditional network appliances in terms of resource sharing and deployment. In contrast to traditional network appliances, virtual switches need to be general enough to perform well on different platforms, without the luxury of specialization [10]. Moreover, virtual switches have to share resources and workloads with the virtualization layer and the VMs.

A virtual switch has two main components: control and data plane. The control plane handles management and configuration, i.e., the administration of the virtual switch (e.g., configuring ports, policies, etc.). The data plane is responsible for forwarding. This functionality can be spread across the system running the virtual switch. The virtual switch can, but does not have to, be separate processes. Moreover, it can either fully reside in user- or kernel-space, or be split across them.

Forwarding is usually based on a sequential (or circular) packet processing pipeline. The pipeline starts by parsing the packet’s header to extract the information that is required for a lookup of the forwarding instructions for that packet. The lookup is typically a (flow) table lookup—the second stage of the pipeline. The final stage uses this result to either forward the packet, drop it, or send it back to the first stage.

### 2.3 Open vSwitch

Open vSwitch (OvS) [9, 10, 22, 23] is a popular open source SDN and multi-platform virtual switch. It meets the high performance requirements of production environments as well as the programmability demanded by network virtualization. OvS is the default virtual switch of OpenStack, Xen, Pica8, and an array of other software systems. OvS’s database can be managed by the switch’s controller via the OVSDB protocol.

OvS uses two forwarding paths: the slow path—a user-space daemon (ovs-vswitchd) and the fast path—a datapath kernel module (openvswitch.ko). OvS can take advantage of a hardware switch for the fast path (e.g., Pica8) [24]. Ovs-vswitchd installs rules and associated actions on how to handle packets in the fast path, e.g., forward packets to ports or tunnels, modify packet headers, sample packets, drop packets, etc. When a packet does not match a rule of the fast path, the packet is sent to ovs-vswitchd, which then determines, in user-space, how to handle the packet. It then passes the packet back to the datapath kernel module to execute the action.

To improve performance for future packets, flow caching is used. OvS supports two main flavors of flow caching: microflow caching and megafow caching. Oversimplifying things slightly, the former builds rules for individual connections, while the latter relies on generalization: It automatically determines the most general rule for handling a set of microflows. The latter can significantly reduce the number of required rules in the fast path. A high-level overview of OvS’s architecture is shown in Figure 2.

### 2.4 MPLS

As our case study takes advantage of the MPLS (MultiProtocol Label Switching) parser, we include a brief overview here. MPLS is often deployed to address the complexity of per packet forwarding lookups, traffic engineering, and advanced path control. MPLS uses

"Forwarding Equivalence Classes" (FECs) to place a “label” in the shim header between the Ethernet and the IP header [25] of a packet, see Figure 3. This label is then used for forwarding. In addition, labels can be stacked via push and pop operations.

An MPLS label is 20 bits long, followed by the Exp field of 3 bits reserved space. This is followed by the 1 bit S field, which, if set to 1, indicates that the label is the bottom of the label stack. It is a critical piece of “control” information that determines how an MPLS node parses a packet. The TTL field indicates the Time-To-Live of the label.

MPLS labels should be under the providers’ administration, e.g., offering L2/L3 VPNs, and are negotiated using protocols such as LDP (Label Distribution Protocol) [26]. As per RFC 3032, MPLS labels are inherently trusted.

### 3 SECURITY ANALYSIS

In this section, we present a systematic security analysis of virtual switches. Based on these insights, we first investigate existing threat models for virtual switches and then construct an attacker model against which virtual switches must be resilient.
3.1 Attack Surface and Vulnerabilities

In the following we characterize the attack surface and vulnerabilities of virtual switches which make them feasible, attractive, and exploitable targets. An overview of the security analysis and the implications is illustrated in Fig. 4.

**Hypervisor co-location:** The design of virtual switches co-locates them—in SDN cloud setups—with the Host system and at least partially with the Host’s kernel, see Figure 2. Components of the virtual switch slow-path often run with elevated (root) privileges in user-space on the Host system. From a performance perspective this is a sensible choice. However, from a security perspective this co-location and elevated privilege puts all virtual machines of the hypervisor at risk once an attack against the virtual switch is successful. Recall, such VMs include those that run critical cloud software, e.g., the VM hosting the controller.

**Centralized control via direct communication:** In an SDN the controller is tasked with all control plane decisions for every data plane component. Hereby, the controller uses its “southbound interface”, today most often “OpenFlow”, to communicate with all data plane elements—here the virtual switches. In a data center following industry best practises this is often implemented using a trusted management network that is shared by all the data plane elements. This implies that a compromised data plane component can directly send packets towards the controller and/or all other data plane elements. Management networks, containing only trusted components, are commonly not protected with an additional intrusion detection system.

**Unified packet parser:** Once a virtual switch receives a packet it parses its headers to determine if it already has a matching flow rule. If this is not the case it will forward the packet to an intermediate entry from the controller. Parsing is the switch’s responsibility as any daemon for the parsed protocol. Alternatively, the attacker can change other cloud resources, e.g., the VM hosting the controller.

**Trusted input:** Virtual switches are commonly deployed in data centers at the network edge. This implies that virtual switches receive network packets directly from the virtual machines, typically unfiltered, see Section 2.3. This can be abused by an attacker. She can—via a virtual machine—send arbitrary data to a virtual switch. Indeed, the virtual switch is typically the first data plane component to handle any packet from a VM. This enables attackers to take advantage of data plane vulnerabilities in virtual switches.

---

3.2 Attacker Models for Virtual Switches

With these vulnerabilities and attack surfaces in mind, we revisit existing threat models. We particularly focus on work starting from 2009 when virtual switches emerged into the virtualization market. We find that virtual switches are not appropriately accounted for in existing threat models, which motivates us to subsequently introduce a new attacker model.

**Existing threat models:** Virtual switches intersect with several areas of network security research: Data plane, network virtualization, software defined networking (SDN), and the cloud. Therefore, we conducted a qualitative analysis that includes research we identified as relevant to attack models for virtual switches in the cloud. In the following we elaborate on that.

Qubes OS [28] in general assumes that the networking stack can be compromised. Similarly, Dhawan et al. [29] assumed that the Software Defined Network (SDN) data plane can be compromised. Jero et al. [30] base their assumption on a malicious data plane in an SDN on Pickett’s BlackHat briefing [31] on compromising an SDN hardware switch.

A conservative attacker model was assumed by Paladi et al. [32] who employ the Dolev-Yao model for network virtualization in a multi-tenant cloud. Grobauer et al. [33] observed that virtual networking can be attacked in the cloud without a specific attacker model.
Jin et al. [34] accurately described two threats to virtual switches: Virtual switches are co-located with the hypervisor; and guest VMs need to interact with the hypervisor. However, they stopped short of providing a concrete threat model, and underestimated the impact of compromising virtual switches. Indeed at the time, cloud systems were burgeoning. However, only recently Alhebaishi et al. [35] proposed an updated approach to cloud threat modelling wherein the virtual switch was identified as a component of cloud systems that needs to be protected. However, in both cases, the authors overlooked the severity, and multitude of threats that apply to virtual switches.

Motivated by a strong adversary, Gonzales et al. [36], and Karmakar et al. [37] accounted for virtual switches, and the data plane. Similarly Yu et al. [38], Thimmaraju et al. [39] and Feldmann et al. [40] assumed a strong adversarial model, with an emphasis on hardware switches, and the defender having sufficiently large resources.

Hence, we posit that previous work have either assumed a generic adversary model for the SDN data plane, stopped short of an accurate model for virtual switches, undervalued the impact of exploiting virtual switches, or assumed strong adversaries. Given the importance and position of virtual switches in general, and in SDN-based clouds in particular, we describe an accurate, and suitable attacker model for virtual switches in the following.

A new attacker model: Given the shortcomings of the above attacker models, we now present a new attacker model for virtual switch based cloud network setups that use a logically centralized controller. Contrary to prior work we identify the virtual switch as a critical core component which has to be protected against direct attacks, e.g., malformed packets. Furthermore, our attacker is not supported by a major organization (she is a “Lone Wolf”) nor does she have access to special network vantage points. The attacker’s knowledge of computer programming and code analysis tools is comparable to that of an average software developer. In addition, the attacker controls a computer that can communicate with the cloud under attack.

The attacker’s target is a cloud infrastructure that uses virtual switches for network virtualization. We assume that our attacker has only limited access to the cloud. Specifically, the attacker does not have physical access to any of the machines in the cloud. Regardless of the cloud delivery model and whether the cloud is public or not, we assume the attacker can either rent a single VM, or has already compromised a VM in the cloud, e.g., by exploiting a web-application vulnerability [41].

We assume that the cloud provider follows security best-practices [27]. Hence, at least three isolated networks (physical/virtual) dedicated towards management, tenants/guests, and external traffic exist. Furthermore, we assume that the same software stack is used across all servers in the cloud.

We consider our attacker successful, if she obtains full control of the cloud. This means that the attacker can perform arbitrary computation, create/store arbitrary data, and send/receive arbitrary data to all nodes including the Internet.

4 CASE STUDY: OVS IN OPENSTACK

Based on our analysis, we conjecture that current virtual switch implementations are not robust to adversaries from our attacker model. In order to test our hypothesis, we conducted a case study. The point we want to make in the following is not that vulnerabilities exist even in well-maintained production software, which is well-known. Rather, our main observation and concern is that finding vulnerabilities can be easily accomplished by amateurs, e.g., by fuzzing; moreover, a single vulnerability can have a devastating impact.

For the purpose of our case study, we evaluate the virtual switch Open vSwitch in the context of the cloud operating system OpenStack against our attacker model. We opted for this combination as OpenStack is one of the most prominent cloud systems, with thousands of production deployments in large enterprises and small companies alike. Furthermore, according to the OpenStack Survey 2016 [18], over 60% of OvS deployments are in production use and over one third of 1000+ surveyed core clouds use OvS.

4.1 Attack Methodology

We conduct a structured attack targeted at the attack surface identified in our analysis.

1. Attack surface analysis: The first step of our analysis is validating co-location assumptions of OvS. We find that by default OvS is co-located with Dom0's user- and kernel-space, see Figure 2. Furthermore, the OvS daemon (ovs-vswitchd) has root privileges. Second, OvS supports logically centralized control and OpenFlow. See Section 2.3 for a more in-depth discussion of OvS. Finally, OvS implements a unified packet parser in its key_extract and flow_extract functions in the fast-past and slow-path resp.

2. Vulnerability identification: Based on our security analysis, we expect to find vulnerabilities in the unified packet parser of OvS. Hence, we used an off-the-shelf coverage-guided fuzz tester, namely American Fuzzy Lop (AFL), on OvS’s unified packet parser in the slow-path. Specifically, for our tests we used AFL version 2.03b, source code of OvS version 2.3.2 recompiled with AFL instrumentation and the test-flows test case[42]. Following common best practice for fuzzing code, all crashes reported by the fuzzer were triaged to ascertain their root cause.

3. Large-scale compromise: The pure presence of a vulnerability is not sufficient to state that OvS is not robust against our threat model. We have to demonstrate that the vulnerability does enable a large-scale compromise. Thus, we need to turn the vulnerability into an exploit. Here, we use a common exploit technique, namely Return Oriented Programming (ROP) [43], to realize a worm that can fully compromise an OpenStack setup within minutes.

4.2 Identified Vulnerabilities

Using the above methodology, we identify several vulnerabilities in the unified packet parser of OvS (ovs-vswitchd). In this paper we only focus on one of the vulnerabilities we found in the stable branch (v2.3.2), as it suffices to demonstrate the attack. Further vulnerabilities discovered during our study include exploitable parsing errors leading to denial of service (DoS) (CVE-2016-2074) and an ACL bypass vulnerability (CVE-2016-10377) in the packet filter component of OvS.
The vulnerability is a stack buffer overflow in the MPLS parsing code of the OvS slow-path. We acknowledge that stack buffer overflows and how they are exploited are well understood. However, we fully document it here to: (i) Underline how easily such vulnerabilities can occur, especially in software handling network packets, and, (ii) To make our work more accessible in the context of networking research outside the security community.

The stack buffer overflow occurs when a large MPLS label stack packet that exceeds a pre-defined threshold is parsed. As predicted, this attack has its root-cause in the unified packet parser for MPLS. Indeed, we note that the specification of MPLS, see RFC 3031 [44] and RFC 3032 [25] does not specify how to parse the whole label stack. Instead, it specifies that when a packet with a label stack arrives at a forwarding component, only the top label must be popped to be used to make a forwarding decision. Yet, OvS parses all labels of the packet even beyond the pre-allocated memory range for that stack. If MPLS would be handled correctly by OvS, it would only pop the top label, which has a static, defined size. Thus, there would be no opportunity for a buffer overflow.

4.3 Exploiting the Vulnerability as a Worm
Following our methodology, the next step is to show how the discovered vulnerability can be used by an attacker to compromise a cloud deployment. We start using the vulnerability to enable code execution on the virtual switch’s host. Subsequently, we extend this to create a worm.

**Exploit:** The next step towards a full compromise is a remote-code-execution exploit based on the discovered vulnerability. We implement this by creating a ROP [43] attack hidden in an MPLS packet. By now, ROP attacks are well documented and can be created by an attacker who has explored the literature on implementing ROP attacks. This is feasible for an average programmer, e.g., using RopGadget [45]. ROP attacks re-combine instruction sequences (called gadgets) from a (target) binary to execute (arbitrary) code. A gadget typically consists of one or more operations followed by a return instruction. After executing each gadget, the return will pop the address of the next gadget into the instruction pointer. The sequence of gadgets that facilitate the execution of (desired) code is called a ROP chain. Given a stack buffer overflow, the attacker overwrites the stack frame with such a ROP chain. Restoration of the overwritten return instruction pointer diverts the control flow of the target program to the first gadget. Once control reaches a return instruction, the next attacker controlled address will be loaded into the instruction pointer.

Recall from Figure 3 that the MPLS label processing terminates if the S bit is set to 1. Therefore, to obtain a successful ROP chain, we select appropriate gadgets by customizing Ropgadget and modify the shell command string. The constraint on the S bit for the gadgets in the MPLS labels is shown in Fig. 5 as the gray lines.

Figure 5 also depicts the ROP chain in our exploit packet, starting with the Ethernet header and padding, followed by the MPLS labels. Our example ROP payload connects a shell on the victim’s system (the server running ovs-vswitchd) to a listening socket on the remote attacker’s system. To spawn the shell the payload triggers the execution of the `cmd` bash `-c "bash -i >& /dev/tcp/<IP>/<PORT> @>&1"` through the `execve` system call (0x3b). This requires the following steps: 1) Set-up the shell command (cmd) string in memory; 2) construct the argument vector `argv`; 3) place the address of the command string in the register `%rdi`; 4) place the address of `argv` in `%rsi`; 5) place the address of `enp` in `%rdx`; 6) place the system call number 0x3b in `%rax`; and finally 7) execute the system call, `execve`.

In summary, our exploit could also have been created by an attacker with average programming skills who has some experience with this kind of technique. This is in accordance with our attacker model, which does not require an uncommonly skilled attacker.

**Worm Implementation:** We need multiple steps to propagate the worm. These are visualized in Figure 6. In Step 1, the worm originates from an attacker-controlled (guest) VM within the cloud and compromises the host operating system (OS) of the server via the vulnerable packet processor of the virtual switch. Once she controls the server, she patches `ovs-vswitchd` on the compromised host, as otherwise the worm packet cannot be propagated. Instead the packet would trigger the vulnerability in OvS yet again.

With the server under her control the remote attacker, in Step 2, propagates the worm to the server running the controller VM and compromises it via the same vulnerability. The centralized architecture of OpenStack requires the controller to be reachable from all servers via the management network and/or guest network. By gaining access to one server we gain access to these networks and, thus, to the controller. Indeed, the co-location of the data plane and the controller, provides the necessary connectivity for the worm to propagate from any of the servers to the controller. Network isolation using VLANs and/or tunnels (GRE, VXLAN, etc.) does not prevent the worm from spreading once the server is compromised.
4.5 Summary

Our case study demonstrates how easily an amateur attacker can compromise the virtual switch, and subsequently take control of the entire cloud in a matter of minutes. This can have serious consequences, e.g., amateur attackers can exploit virtual switches to launch ransomware attacks in the cloud. This is a result of complex packet parsing in the unified packet parser, co-locating the virtual switch with the virtualization layer, centralized and direct control, and inadequate attacker models.

5 DISCUSSION: ANALYSIS OF RELATED TECHNOLOGIES

While so far we were mainly concerned with virtual switches (and in particular OvS in our case study), we believe that our work has ramifications far beyond. Our general observations apply not only to virtual switches across the board, but also to emerging NFV implementations and high-performance fast path implementations. Hence, in this section we evaluate, which other implementations and data-plane component classes are affected by our analysis. See Table 1 for a summary of our observations for some representative examples from each group.

High Performance Fast Paths: High performance fast paths (HPFPs) are software libraries for handling packet forwarding in user-space. Prominent examples include Data Plane Development Kit (DPDK) [67, 68] and NetMAP [47]. HPFPs try to minimize the performance bottlenecks of packet forwarding in the kernel. They accomplish this, by, e.g., using large page sizes, dedicated ring buffers, uniform packet format sizes, and improved buffer management. Thus, HPFPs can be used to increase forwarding performance in user-space virtual switches by eliminating the kernel (fast-path), e.g., OvS with DPDK [69].

Besides increasing virtual switch performance, an HPFP also increases security as it reduces packet processing in the kernel. This reduces the attack surface but does not fully address the problem of co-location since it is still running on the same host OS as the hypervisor. Moreover, we find that some HPFPs are not designed with software security in mind. Only IX [49] and Arrakis [48] are designed with the goal of improving packet handling security. NetMAP [47] at least discusses that not using shared memory with the host’s kernel improves security. Furthermore, software mitigations to limit the impact of vulnerabilities are not used by either of them.

Virtual Switch Implementations: Our comparison of virtual switches in Table 1 uses OvS as the baseline. Competing commercial virtual switch products include Cisco’s Nexus 1000V [11], the VMware vNetwork [12], Microsoft Hyper-V vSwitch [54] and Microsoft VFP [2]. These implementations suffer from the same conceptual issues that we identified in our attack surface and verified with OvS due to hypervisor co-location [10, 70]. Since they are closed-source software systems, we do not know specifics about their use of software mitigations. Notably, Microsoft VFP introduces middlebox functionality into their virtual switch thereby increasing the susceptibility due to parsing. Lagopus, another open-source virtual switch implementation lacks the same popularity as OvS, yet retains its design shortcomings [56].
Research projects in the area of virtual switches, e.g., Vale [52] and NetVM [55], are mainly focused on performance. Thus, they often rely on HPFPs. This decreases their co-location attack surface in comparison to plain OvS. However, since they commonly still use kernel modules and/or user mode components with elevated privileges, the principle attack vector is still there. Thus, using HPFPs does not have a significant impact on the security of such designs. Furthermore, to support, e.g., OpenFlow, they have to implement extended parsers for packet content. In contrast to the above projects we find that PISCES [62] reduces the attack surface by increasing performance. Yet, its design focus on flexibility and extensibility increases the attack surface again. Similarly, fd.io uses Vector Packet Processing, e.g., see Choi et al. [58], to handle packets, e.g., in between containers, but also as an interface to conventional data-plane components. Yet, again, this packet processing and parsing component lacks security considerations and remains co-located with critical host components. Overall, we find that academic virtual switch proposals rarely focus on security or evaluate software mitigations for their virtual switch designs.

**Network Function Virtualization:** Network Function Virtualization (NFV) is a relatively new trend, whereby data plane network functions such as routers, firewalls, load balancers, intrusion detection systems, and VPN tunnel end-points are moved from specialized devices to VMs. With SDNv2 [71], NFVs get folded into SDN via Virtualized Network Functions (VNFs). Here, VNFs are network function implementations that commonly use a virtual switch and add their functionality on top, decoupled from the underlying hardware. In principle, network functions need more complex parsing and processing. Hence, their attack surface is larger. Moreover, we find that some NFV/VNF frameworks are built on top of OvS as their virtual switch component. Thus, they suffer from the same attack vectors as OvS. Some proposals, e.g., such as EDEN [65], go a step further and suggest to move network functions to all end-hosts. Therefore, such proposals increase the attack surface by increasing the number of possibly affected systems. Moreover, none of the NFV solutions included in Table 1 consider software mitigations or have their focus on security.

For SDN, virtual switches are again central components. Moreover, we note that most current proposals of the SDN community, e.g., Open Virtual Network (OVN) [66], suggest to co-locate the SDN controller with the virtualization layer and data plane components. Thus, SDN is highly susceptible to the attack surface pointed out in this paper. With recursively virtualized SDNs [72] this attack surface will be increased even further.

**Summary:** Emerging technologies for improving performance of user-space fast-path packet processing slightly reduce the attack surface pointed out in this paper. However, contemporary virtual switches not employing HPFPs suffer from the same problems as we demonstrated in OvS. The root-cause lies in the shared architecture of such virtual switches that co-locates them (partially) with the host system. In addition, new technologies like NFV are also affected. Similar to OvS, these technologies are commonly implemented across user- and kernel-space. In addition, these technologies heavily rely on parsing, e.g., in case of DPI and load balancing. Proposals such as EDEN even consider implementing such NFV components on all end-hosts, spreading the attack surface further. Finally, we find that software mitigations are typically not evaluated when designing data plane components, as the main focus is on performance rather than security.

### Table 1: Attack surface summary for HPFPs, virtual switches, and SDN/NFV example implementations.

<table>
<thead>
<tr>
<th>Name</th>
<th>Ref.</th>
<th>Year</th>
<th>OvS based</th>
<th>Co-Location</th>
<th>Ext Parsing</th>
<th>SOFA Mitigations</th>
<th>Sec. Enum.</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>HPFP</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>HPFP</td>
<td>[46]</td>
<td>2011</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>NetMAP</td>
<td>[47]</td>
<td>2012</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Arrakis</td>
<td>[48]</td>
<td>2014</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>IX</td>
<td>[49]</td>
<td>2014</td>
<td></td>
<td></td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ESWITCH</td>
<td>[50]</td>
<td>2016</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Virtual Switches</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>OvS</td>
<td>[51]</td>
<td>2009</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Baseline</td>
</tr>
<tr>
<td>Cisco NexusV</td>
<td>[1]</td>
<td>2009</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>VMware vSwitch</td>
<td>[12]</td>
<td>2009</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Yale</td>
<td>[52]</td>
<td>2012</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>HyperSwitch</td>
<td>[53]</td>
<td>2013</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td>✓</td>
<td>Using HPFP to increase performance</td>
</tr>
<tr>
<td>MS HyperV-Switch</td>
<td>[54]</td>
<td>2013</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td>✓</td>
<td>Using HPFP to increase performance</td>
</tr>
<tr>
<td>NetVM</td>
<td>[55]</td>
<td>2014</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Using HPFP to increase performance</td>
</tr>
<tr>
<td>Lagopus</td>
<td>[56]</td>
<td>2014</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Different vSwitch with a featureset similar to OvS</td>
</tr>
<tr>
<td>Id.io</td>
<td>[57]</td>
<td>2015</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Uses Vector Packet Processing, e.g., see Choi et al. [58]</td>
</tr>
<tr>
<td>mSwitch</td>
<td>[59]</td>
<td>2015</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Using HPFP to increase performance</td>
</tr>
<tr>
<td>RESS</td>
<td>[60]</td>
<td>2015</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Similar to the Click modular router [61]</td>
</tr>
<tr>
<td>PISCES</td>
<td>[62]</td>
<td>2016</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td>✓</td>
<td>Uses a domain specific language to customize parsing</td>
</tr>
<tr>
<td>SDN/NFV</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Unify</td>
<td>[63]</td>
<td>2014</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td>NFV Chaining</td>
</tr>
<tr>
<td>ClickDS</td>
<td>[64]</td>
<td>2014</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Places a software switch on virtualization host</td>
</tr>
<tr>
<td>EDEN</td>
<td>[65]</td>
<td>2015</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Places EDEN on end-hosts; Parses more to enable NF</td>
</tr>
<tr>
<td>OVN</td>
<td>[66]</td>
<td>2015</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td>✓</td>
<td>Co-locates SDN controller with the hypervisor</td>
</tr>
</tbody>
</table>

Susceptibility to parameters: ✓ less than OvS; ? similar to OvS; > more than OvS; ?: unknown.
Table 2: Size comparison of ovs-vswitchd and openvswitch.ko binaries using gcc countermeasures and grsecurity patch respectively.

<table>
<thead>
<tr>
<th>Binary type</th>
<th>Binary size(MB)</th>
<th>% of Baseline</th>
</tr>
</thead>
<tbody>
<tr>
<td>ovs-vswitchd baseline</td>
<td>1.84</td>
<td></td>
</tr>
<tr>
<td>ovs-vswitchd with stack protector and pie</td>
<td>2.09</td>
<td>+13.59%</td>
</tr>
<tr>
<td>openvswitch.ko baseline</td>
<td>0.16</td>
<td></td>
</tr>
<tr>
<td>openvswitch.ko with grsecurity</td>
<td>0.21</td>
<td>+31.25%</td>
</tr>
</tbody>
</table>

6 SOFTWARE COUNTERMEASURES

There exist many mitigations for attacks based e.g., on buffer overflows, including MemGuard [73], control flow integrity [74], position independent executables (PIEs) [75], and Safe (shadow) Stack [76]. Any one of these severely reduces the impact of crucial, frequently occurring vulnerabilities like the one used as an example in this paper. However, due to their assumed performance overhead, especially on latency, they are commonly not deployed for virtualized network components.

Hence, while these mitigations are widely available, we find that they are not enabled by default for OvS. Furthermore, virtual switch solutions presented in the literature commonly do not discuss these techniques. One possible downside of these mitigations is their performance overhead. Past work reported that MemGuard imposes a performance overhead of 3.5–10% [73] while PIEs have a performance impact of 3–26% [75]. Furthermore, prior evaluations did not focus on the systems’ network performance. Instead, their main focus was on the systems’ process performance, e.g., kernel context switches and the size of compiled binaries with the applied mitigations. However, in the context of OvS, network related metrics are far more relevant: Forwarding latency and forwarding throughput.

In order to investigate the potential performance penalty of such countermeasures, we showcase two variants of these mitigation techniques that are supported by the Gnu cc compiler gcc out of the box. Namely, stack protector and position independent executables. To determine the practical impact of these mitigations, we designed a set of experiments to evaluate the performance impact on OvS’s forwarding latency and throughput.

Evaluation Setup: The test setup is chosen to ensure accurate one-way delay measurements. Thus, for our tests, we use three systems, all running Linux kernel (v4.6.5) compiled with gcc (v4.8). The systems have 16GB RAM, two dual-core AMD x86_64 2.5GHz, and four Intel Gigabit NICs. The systems are interconnected as follows: One system serves as the Load Generator (LG) and replays packet traces according to the specific experiments using tcpreplay. This system is connected to the Device Under Test (DUT), configured according to the different evaluation parameters. The data is then forwarded by OvS on the DUT to a Load Receiver (LR), a third system.

The connections between LG and DUT, and, LR and DUT respectively are monitored via a passive taping device. Both taps are connected to our measurement system. This system has two dual-core Intel(R) Xeon(TM) CPUs running at 3.73GHz with hyperthreading enabled and 16GB RAM. We use an ENDACE DAG 10X4-P card to capture data. Each line (RX/TX) of the tapped connections is connected to one interface of the DAG 10X4-P. Each interface has its own receive queue with 1GB. This ensures accurate one-way delay measurements with a high precision, regardless of the utilization of the measurement host.

Evaluation Parameters: We evaluate forwarding latency and throughput for eight different combinations of traffic composition and software mitigations. We compare a vanilla Linux kernel (v4.6.5) with the same kernel integrated with grsecurity patches (v3.1), which protects the in-kernel fast-path by preventing kernel stack overflow attacks using stack canaries, address space layout randomization and ROP defense. For both kernels, we evaluate two versions of OvS-2.3.2: The first one compiled with -fstack-protector-all for unconditional stack canaries and -fpie for position independent executables; the second one compiled without these two features. Since gcc, the default compiler for the Linux kernel, does not support Safestack (safe and unsafe stack) we did not evaluate this feature, even though it will be safe with clang, another compiler, starting with version 3.8. As Table 2 shows, the selected mitigations increase the total size of the ovs-vswitchd and openvswitch.ko binaries significantly. However, apart from embedded systems, the size changes are not relevant on modern systems with several hundred gigabytes of memory.

One important feature in virtual switches, recall Section 2, is, whether traffic is handled by the slow or the fast path. We decided to focus on the corner cases where traffic is either handled exclusively by the fast or by the slow path. By isolating the two cases we can assess if and to what extent the software security options impact each path. Hereby, we follow current best practices for OvS benchmarking, see Pfaff et al. [10]. To trigger the slow path for all packets in our experiments, we disable the megafloes cache and replay a packet trace in which each packet has a new source MAC address (via sequential increments). For measuring fast path performance, we pre-establish a single flow rule on the DUT, a wildcard-one, that matches all packets entering from the LG. The rule instructs the virtual switch to process these packets via the fast path and forward them on the interface connected to the LR. Therefore, for the sake of consistency, we can replay the same traces as used for the slow path experiments. Additionally, to reduce the uncertainty in our setup, we pin ovs-vswitchd to a single core.

Latency Evaluation: For the latency evaluation, we studied the impact of packet size on OvS’s forwarding latency and throughput.

For the latency evaluation, we studied the impact of packet size on OvS forwarding. We selected the following packet sizes from the legacy MTU range: 60B (minimum IPv4 UDP packet size with two bytes of content), 512B (average packet), and 1500B (Maximum Transmission Unit (MTU)) packets. In addition, we also select the following jumbo frames: 2048B packets (small jumbo frame) and 9000B (maximum jumbo frame). For each experimental run, i.e., packet size and parameter set, we continuously send 10,500 packets from the LG to the LR via the DUT at a rate of 10 packets per seconds (pps). To eliminate possible build-up or pre-caching effects, we only evaluate the last 10,000 packets of each experiment.

The results for the latency evaluation are depicted in Figures 7a and 7b for the slow path and fast path resp. We find that grsecurity (grsec default and grsec all) imposes a minimal increase in latency for all packet sizes in the slow and fast path. We observe a minimal impact of user-land protection mechanisms, 1-5%, see Figure 7a, for slow path latency, both, for a vanilla and a grsecurity enabled
Throughput Evaluation: For the throughput evaluation we use a constant stream of packets replayed at a specific rate. We opted for small packets to focus on the packets per second (pps) throughput rather than the bytes per second throughput. Indeed, pps throughput indicates performance bottlenecks earlier [77] than bytes per second. As in the latency experiments, we opted to use packets that are 60B long. Each experimental run lasts for 1000 seconds and uses a specific replay rate. Then we reset the system and start with the next replay rate. Our evaluation focuses on the last 900 seconds. For the slow path, the replay rates start from 10k to 40k packets per second, in steps of 1k pps. For the fast path, the replay rates start from 300k to 900k packets per second, in steps of 10k pps. For better readability we show the slow path plot from 10k to 35k pps.

An overview of the results for the slow and fast path throughput measurements are depicted in Figures 7c and 7d resp. In the slow path, packet loss for the vanilla kernel first sets in just after 18k pps, while the experiments on the gressec enabled kernel already exhibit packet loss at 14k pps. In the fast path, gressec exhibits packet loss from 350k pps whereas the vanilla kernel starts to drop packets at 690k pps. Hence, we note that the gressec kernel patch does have a measurable impact on the forwarding throughput in the slow and fast path of OvS. With respect to the user-land security features, we observe an overhead only in the slow path of approximately 4-15%.

Summary: Our measurements demonstrate that user-land mitigations do not have a large impact on OvS’s forwarding performance. However, gressec kernel patches do cause a performance overhead for latency as well as throughput. Given that cloud systems support a variety of workloads, e.g., low latency or high throughput, kernel-based mitigations may or may not be used. However, cloud systems such as the one studied by Pfaff et al. [10] can adopt the user-land and kernel software mitigations described in this paper.

It is only a question of time until the next wormable vulnerability in a virtual switch is discovered. As software mitigations can be more easily deployed than a fully re-designed virtual switch ecosystem, we strongly recommend the adoption of software countermeasures, until a more securely designed virtual switch platform can be rolled out.

Moreover, our security analysis underlines the need for networking researchers to include software countermeasures in their design, implementation, and evaluation of novel networking components. As indicated by our analysis of related virtual switch network technologies, the networking research community must integrate security considerations into their work on new SDN and NFV technologies.
While we did not implement remote attestation, we argue that their work, in principle, demonstrates the feasibility of this technique, we propose to use integrity measurements to detect irregular behavior. Sensible attestation points are, e.g., at regular time intervals, need a way to reduce the overhead, e.g., by using redundant set of controllers. However, we also beyond the remote attestation of flow tables. However, we can leverage a presumed security weakness (centralized operation) into an opportunity to defend infrastructure from misbehaving (attacker-controlled) nodes.

**Virtualized/Isolated data plane:** One essential feature of the identified attack surface is the co-location of data plane and hypervisor (see Section 3). Addressing this problem in OpenStack is non-trivial due to the sheer number of interacting components and possible configurations, e.g., virtualized/non-virtualized, integrated/distributed, redundant/hierarchical controllers [78].

One way to design a system with stronger separation is to virtualize the data plane components, thereby de-coupling it from the virtualization layer. For virtual switches one example of such a proposal is to shift the position of the virtual switch from the host to a dedicated guest as proposed by Jin et al. [34]. However, the IOMMU of the host must be used to restrict access of the network cards to the network interfaces. Otherwise the physical host and the operating system running there are left vulnerable to direct memory access (DMA) attacks [79]. Such a design reduces the host OS’s Trusted Computing Base (TCB) and, thereby, the attack surface of the virtual switch. We note that Arrakis [48] and IX [49] are promising proposals for HPFPs that would allow for designing such a system. Note, that while Arrakis utilizes the IOMMU, the authors of IX left this for further work.

Furthermore, to reduce the attack surface of hypervisors, Szefer et al. [80] suggest that the hypervisor should disengage itself from guest VMs, and the VM should receive direct access to the hardware (e.g., NIC). In conjunction with our suggestion of transferring the virtual switch into a virtual machine, the approach of Szefer et al. results in a more secure data plane that can no longer attack the hypervisor.

**Data plane (remote) attestation:** By isolating the data plane one can reduce the impact of an attack. Yet, an attacker can still attack other data plane systems from a compromised virtual switch. Here we propose to use integrity measurements to detect irregular behavior of exploited systems. One example of such irregular behavior is our worm, where the ovs-vswitchd binary is modified to propagate malformed MPLS packets.

One existing approach is remote attestation for OVS flow tables, as prototyped by Jacquin et al. [81]. The authors perform remote attestation of an OVS flow table in 953 ms with their prototype. While we did not implement remote attestation, we argue that their work, in principle, demonstrates the feasibility of this technique, also beyond the remote attestation of flow tables. However, we need a way to reduce the overhead, e.g., by using redundant set of OVS switches, since a one second network outage is not practically feasible. Sensible attestation points are, e.g., at regular time intervals, at startup, and after errors.

With an isolated data plane, the hypervisor controls the switching VM. Hence, we can use the hypervisor to enforce control flow integrity (CFI) on this VM. Using this primitive we can guarantee that data plane vulnerabilities at most result in a DoS attack, and the host no longer gets compromised. Isolation of VMs can be done by leveraging an Open-Flow centric IDS architecture such as the one presented by Xing et al. [82] for isolating misbehaving nodes (VMs) in the cloud. Hence, in particular, in the context of SDN we can leverage a presumed security weakness (centralized operation) into an opportunity to defend infrastructure from misbehaving (attacker-controlled) nodes.

**Control plane communication firewalls:** Another method to contain and prevent attacks like the worm is tight firewalling of the control plane. In contrast to “normal” Internet traffic, control plane traffic has characteristics that enable a tighter and more secure firewall design: (i) The control plane traffic volume should be significantly smaller than regular network traffic. (ii) Nodes should only communicate via the controller and not among each other. Hence, there is a central location for the firewall. (iii) On the control channel there should only be the control communication protocol, e.g., the OpenFlow protocol. Even if more protocols are necessary, e.g., Simple Network Management Protocol (SNMP), the list is small, favoring a white-listing approach. (iv) The communication protocol for SDN systems is clearly defined. Hence, in addition to the networking layer checks a strict syntactic white-listing of the control messages is feasible.

Thus, implementing a firewall and/or IDS that intercepts and cleans all control communication appears feasible. Depending on the threat model, one may even opt to chain multiple IDS/firewalls or use physical appliances for such firewalling [40].

### 8 RELATED WORK

**Cloud systems:** In the past, various attacks on cloud systems have been demonstrated. Ristenpart et al. [83] show how an attacker can co-locate her VM with a target VM to obtain secret information. Costin et al. [41] find vulnerabilities in web-based interfaces operated by cloud providers. Wu et al. [84] assess the network security of VMs in computing clouds. They point out what sniffing and spoofing attacks a VM can carry out in a virtual network.

Ristov et al. [85] investigate the security of a default OpenStack deployment and show that it is vulnerable from the inside rather than the outside. Indeed, the OpenStack security guide [27] mentions that OpenStack is inherently vulnerable to insider threats due to bridged domains (Public and Management APIs, Data and Management, etc.).

**SDN security:** At the heart of the software-defined networking paradigm, lies its support for formal policy specification and verification. Thus, it is often believed that SDN has the potential to render computer networking more verifiable [8, 86] and secure [87, 88]. However, several researchers have pointed out security threats for SDN. For example, Klöti et al. [89] report on STRIDE, a threat analysis of OpenFlow, and Kreutz et al. [90] survey several threat vectors that may enable the exploitation of SDN vulnerabilities.

The goal of various projects is to design more robust and secure SDN control planes. For example, Canini et al. suggest transactional network updates, utilizing SDN [91] and methods to test OpenFlow applications [92]. Porras et al. introduce a dedicated kernel for OpenFlow networks that allows the selective enforcement of security policies [87].
So far, work on how to handle malicious switches is sparse. Sonchack et al. describe a framework for enabling practical software-defined networking security applications [93] and Shin et al. [88] present a flow management system for handling malicious switches. Work on compromised data planes is sparse as well. For example, Matsumoto et al. [94] focus on insider threats. Furthermore, national security agencies are reported to have bugged networking equipment [95] and networking vendors have left backdoors open [96–98], leading to additional threats.

Hong et al. [99] focus on how the controller’s view of the network (topology) can be compromised. They identify topology based attacks in an SDN that allow an attacker to create false links to perform man-in-the-middle and blackhole attacks. Furthermore, they propose Topoguard, a defense mechanism to detect and prevent such attacks by verifying the integrity of topology messages (LLDP) as well as changes to the topology based on certain pre- and post-conditions. Although they discovered novel SDN attacks, their threat model does not account for a compromised data plane.

Most proposals rely on the integrity of the network controller. However, we show with our attack that it can be compromised. Moreover, we demonstrate how the whole data and control plane of a cloud setup can be compromised within minutes. This leaves no majority of uncompromised devices.

**Data plane security:** Lee et al. [100] investigate how malicious routers can disrupt data plane operations, while Kamisinski et al. [101] demonstrate methods to detect malicious switches in an SDN. In addition, Perez-Botero et al. [102] characterize possible hypervisor vulnerabilities and identify Network/IO as one. In contrast to our work, they omit a deep analysis on the challenges introduced by co-located data planes. Hence, they did not find any network based vulnerabilities.

Dobrescu et al. [103] develop a data plane verification tool for the Click software. They prove properties such as crash-freedom, bounded execution, or filtering correctness for the switch’s data plane. Hereby, they use compositional symbolic execution to verify whether the data plane implementation satisfies the desired program properties. The authors cleverly side-step the “path explosion” problem inherent to symbolic execution by making their analysis compositional. However, their compositional analysis can only be applied to software implementations (i) that are strictly compositional in nature; (ii) whose packet processing elements share no state among them, other than the processed packet itself; and (iii) that make use of data structures which expose a key/value-store interface and are verifiable themselves, e.g., the Click modular router [61]. Legacy data plane implementations typically do not adhere to these conditions. In fact, OVS’ implementation is not compositional and is not suited for compositional verification due to the high-degree of shared state, e.g., the unified packet parser in OVS is primarily one large function (flow_extract and emplkey_extract in the slow- and fast-path resp.). Although software verification tools can ensure the correctness and security of greenfield software data plane solutions, they currently fall short of ensuring this for legacy software. In such a scenario, coverage guided fuzz testing is a more appropriate approach.

### 9 CONCLUDING REMARKS

In this paper we present our study of the attack surface of today’s virtualized data planes as they are frequently used in SDN-based cloud systems. We demonstrate that virtual switches are susceptible to various attacks by design. The key issues are: (i) Co-location of the virtual switch with the hypervisor, (ii) A central controller which, if compromised, threatens the security of the whole network/data center, (iii) Support for a unified protocol parser in data plane components, and, (iv) Direct exposure of data plane components to crafted attack packets. Furthermore, we point out that existing threat models for virtual switches are insufficient. Accordingly, we derive a new attacker model for (virtualized) data planes and underline this by demonstrating a successful attack against OpenStack which exploits the aforementioned design weaknesses.

Our survey of related data plane technologies including NFV/SDN and other virtual switches finds that they are susceptible to the same security design flaws. Even though HPFPs can be used in virtual switches to improve their design’s security, they are usually only used to increase performance. Furthermore, readily available software security measures in are commonly not evaluated for new data plane components. This is unfortunate, as our evaluation of such techniques indicates that they introduce minor performance overheads. We discuss architectural changes that limit the remaining performance impact of software vulnerabilities. These should be adopted in the long-term, as the number of parsed protocols in virtual switches is still on the rise.

With hardware vendors, e.g., Broadcom and Cavium Networks, selling so-called SmartNICs [104, 105], i.e., NICs running a full fledged virtual switch such as OvS, we believe the attack surface has been extended to the NIC as well. As we demonstrated, neglecting security during the design of virtual switches, SDN, and, NFV data plane components can have dramatic consequences on deployed real-world systems.

### ACKNOWLEDGMENTS

The authors thank the anonymous reviewers for their valuable feedback and comments. The authors would like to express their gratitude towards the German Federal Office for Information Security, for initial discussions on the security of the SDN data plane. This work was partially supported by the Helmholtz Research School in Security Technologies scholarship, Danish Villum Foundation project “ReNet”, BMBF (Bundesministerium für Bildung und Forschung) Grant KIS1DSD032 (Project Enzevalos), and by the Leibniz Prize project funds of DFG/German Research Foundation (FKZ FE 570/4-1). We would also like to thank the security team at Open vSwitch for their timely response. Finally, we thank Jan Nordholz, Julian Vetter and Robert Buhren for their valuable discussions on the software countermeasures.

### REFERENCES


