Security and reliability of SDN — current challenges and perspectives

Andrzej Kamisiński
kamisinski@kt.agh.edu.pl

Faculty of Computer Science, Electronics and Telecommunications
Department of Telecommunications

19.03.2015
Outline

- Introduction
- Different perspectives
- SDN — secure by design?
- Is SDN a reliable networking concept?
- Conclusion
Software-Defined Networking

CONTROL PLANE

Logically-centralized controller

Management, Applications

OpenFlow

DATA PLANE

Network node

Network node

Network node

Network traffic
Software-Defined Networking (cont.)

- Separation of the *control plane* from the *data plane*
- The OpenFlow protocol (2008)
- Independent hardware and software modules
  - One software distribution, different hardware vendors
  - Network-wide deployment of new features
- Highly flexible networking concept
- Lower management cost (programmable network services)
"The goal is to provide effective communications and services where network, data, and computation are fused into a service architecture."

One framework, different perspectives

- Wired/wireless computer networks
- Wireless sensor networks
- Carrier infrastructure
- Local networks
- Data center networks, cloud computing
- Cellular Radio Access Networks, 5G networks
- SDX — Software-Defined Exchange
- Smart grid communications
- ...
SDN security — challenges

- Complexity of management protocols (OpenFlow)
- Avoiding software defects (programmers’ errors)
- Different implementations of software modules
- Malicious software
Client-switch, switch-controller, controller-controller, application-controller and administrator-controller communications
Authentication and authorization mechanisms
Intrusion detection and prevention systems
Attackers pretending to be switches or controllers (spoofing)
SDN security — challenges (cont.)

- Manipulation of the node configuration
- Disrupting, modifying or injecting network traffic
- DDoS attacks against network nodes
  - Input buffer overflow
  - Switches forward the entire packets to the controller
  - Limited capacity of the flow table
- The attackers know how to use the OpenFlow protocol to interact with the controller
Defining a reasonable security policy and enforcing it in the network

Interaction with legacy (non-SDN) equipment

Information disclosure

The OpenFlow standard does not require a notification in case of counter overflow, nor does it provide a method with which this could be done

TLS is not mandatory (switch-controller)

Maintenance of the PKI
SDN security — threat vectors map

1. SDN node
2. SDN node
3. SDN node
4. SDN Controller
5. Application
6. Administrator's station
7. Network traffic

CONTROL PLANE

DATA PLANE

OpenFlow

Client
Forged or faked traffic flows

- Faulty devices
- Malicious activity
- Attacks against other SDN devices possible (including the controller)
Attacks on vulnerabilities in switches

- Dropping packets
- Forwarding packets to wrong destinations
- Injecting traffic into the network
- Information disclosure
- Sending forged requests to the controller
Attacks on control plane communications

- Information disclosure
- DoS attacks
- Security of the TLS implementation
- Providing false reports to the controller
Attacks on and vulnerabilities in controllers

- Information disclosure
- The entire network may be compromised
There are no mechanisms to ensure that the application is to be trusted

The entire network may be compromised
The entire network may be compromised

Possible infection via external devices (USB, ...), side-channel attacks
Forensics and remediation

- Data collection and analysis
- No predefined trusted resources
- Intrusion detection and prevention
SDN reliability

- Availability of network services
- Quality of Service
- Relation between the SDN architecture and the forwarding infrastructure
- Maintaining the proper network operation in the presence of various threats
Replication

- Multiple instances of network controllers
- Application instances on different controllers
- Location-based attacks
- Masking hardware and software failures
Diversity

- Similar devices from different vendors are less likely to have common errors
- Reducing the impact of hardware and software faults
- Common approach in mission-critical systems (DNS, ...)

A. Kamisiński (AGH-UST) Security and reliability of SDN 2015 21 / 30
Self-healing mechanisms

- Detecting abnormal behavior in the network
- Replacing the suspicious devices with pre-configured trusted instances
- Maintaining the diversity across the entire network
Dynamic device association

- One switch, multiple controllers
- Failure of one controller does not block the communication
- Load balancing opportunities
- Reducing control delay
Fast and reliable software update and patching

- Removing software errors
- Network-wide deployment of new features
- Common software distribution, reduced management cost
Region-based failures

- Backup network topologies
- Fast restoration techniques


- Logically-centralized SDN controller (physical locations, number of instances, assignment of nodes to the controller instances)

One framework, different perspectives...

- Mission-critical or low-importance infrastructure
- Different propagation media
- Static nodes or mobile terminals
- Acceptable QoS levels (throughput, delay, jitter, ...)
- Interaction with legacy network equipment
- ...

A. Kamisiński (AGH-UST) Security and reliability of SDN 2015 26 / 30
Conclusion

- An extensive use of software components introduces the risk related to errors and new vulnerabilities
- The SDN concept is not secure by design and requires that additional security measures be employed in a network
- The original proposal can be extended to provide better reliability
References


Recommended reading


Thank you for your attention!

Andrzej Kamisiński
kamisinski@kt.agh.edu.pl