SDN security
Nokia Research perspective

Peter Schneider
19-05-2015
Version 1.1
Agenda

- Security at Nokia
- SDN in mobile networks
- SDN security research
- SDN security standardization
- Securing SDN based networks
- Using SDN to implement security solutions
- Conclusion: SDN security challenges and opportunities
Security at Nokia

- Product security
  - security processes
  - “security leads” per product
  - “security managers” per product line
  - central product security team
- Security products (including services)
- Security Research: Teams in Munich and Espoo (~20 people)
- Security Experts in various functions (e.g. standardisation)
Nokia Security building blocks

Security Services
Technical Consulting

Radio Access Security

Core Network Security

End User Security

Security Ecosystem: Nokia and qualified partner security products

Secure Network Elements: Design for Security
Nokia’s mobile network security vision
Summary of Research areas

1. Embedded security for 5G
2. Intelligent monitoring & response
3. Improving the security foundation
4. Easy security management & usability
5. Tool supported co-operation
The evolved packet system (4G mobile network)

- Control plane
- User plane
- Control+user plane
- Trusted
- Untrusted
- Internet
- Corporate IP networks
- Don’t care about all these abbreviations!
Control functions move into the cloud
Gateways may be split into control and forwarding part
Work on SDN security at Nokia Research

• Interacting with the research community
• Own research
  - understand the SDN security issues
  - solution sketches for Nokia products/services including SDN
  - intellectual property rights
  - internal/external research papers/presentations
• Monitoring/supporting SDN standardisation
• Monitoring the market (commercial SDN products)
• Nokia internal enabling; ultimate goal is to create secure innovative products
Monitoring the SDN security research community – examples (1/3)


• Further valuable vulnerability analyses in
  but mitigation measures given in [5] seem cumbersome in practice

Monitoring the SDN security research community – examples (2/3)

• Valuable contributions by the research team OpenFlowSec.org (see http://www.openflowsec.org/Home.html):
  - Security enhanced OpenFlow controllers FortNOX and SE-Floodlight: Ensure secure access of applications to network resources, provide patterns simplifying the programming of threat mitigation measures (see [7] and [8])
  - FRESCO: “an OpenFlow security application development framework designed to facilitate the rapid design, and modular composition of OF-enabled detection and mitigation modules” [9]

• Access control for applications via the SDN controller
Monitoring the SDN security research community – examples (3/3)

• Improving security techniques by SDN
  - S. A. Mehdi et al., “Revisiting traffic anomaly detection using software defined networking” [12]

• Network virtualization (and isolation) using SDN:
SDN security research in SASER-SIEGFRIED

• SASER (Safe and Secure European Routing) (https://www.celticplus.eu/project-saser/):
  - Celtic-Plus project with national funding in Germany, France, Finland
  - a large project in Germany: three divisions led by different vendors, 36M € funding
  - originally an optics project, but with security focus; 3 years runtime (2012-2015)
  - SASER-SIEGFRIED: one of the German divisions of SASER, led by Nokia, with a substantial work package on security, including SDN security

• SDN security work in SASER-SIEGFRIED
  - SDN security basics (threats, protection measures)
  - concepts to control the interaction of multiple applications on an SDN controller
  - SDN security lab, PoC implementations of security for southbound and northbound interface, admission control system for applications
  - publications, e.g. C.Röbke, T.Holz, “Retaining Control Over SDN Network Services” [16]
  - SDN demos including security features, see S. Gebert, et al., “Demonstrating the Optimal Placement of Virtualized Cellular Network Functions in Case of Large Crowd Events” [17]
### Monitoring SDN security standardization: ONF

<table>
<thead>
<tr>
<th>SDN Architecture document:</th>
<th>Reasonable (high level) statements on security</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>ONF specifications (examples):</strong></td>
<td></td>
</tr>
<tr>
<td>- OF-Switch: Optional use of TLS, no TLS-profile specified</td>
<td></td>
</tr>
<tr>
<td>- OF-Config: Based on NetConf → security using SSH or TLS</td>
<td></td>
</tr>
<tr>
<td><strong>ONF Principles document:</strong></td>
<td></td>
</tr>
<tr>
<td>- First output of the ONF Security Project (after a slow start as “Security Discussion Group”)</td>
<td></td>
</tr>
<tr>
<td>- 8 rather generic security principles, 24 security requirements</td>
<td></td>
</tr>
<tr>
<td>- Reasonable recommendations how to improve the security of OF-Switch</td>
<td></td>
</tr>
<tr>
<td>- What will be the impact of this work?</td>
<td></td>
</tr>
</tbody>
</table>

**Overall, the ONF security work appears somewhat immature.**
Monitoring SDN security standardization: Others

**IRTF SDN research group**: Security as a “field of interest” in the charter, but no output so far (?). Discussions at IETF#92 how to move on with the group.

**IETF SDN related WGs (examples)**:
- ForCES: Use secure transport protocol between forwarding and control plane, e.g. SCTP/IPsec; programmability of the network not in scope
- I2RS: Reasonable security requirements for the interface; could be based on NetConf → security using SSH or TLS
- A new activity: I2NSF (“interface to network security functions”)

**ETSI ISG NFV**: SDN usage in NFV covered in EVE (Evolution and Ecosystem) group; early draft “Report on SDN Usage in NFV Architectural Framework”; security aspects not yet elaborated; also no respective work item in the NFV SEC (Security) group
Threats to an SDN-based network

- Attacks from the forwarding plane
- Attacks from the control network
- Attacks via the northbound interface
- Attacks from the virtualized/cloud environment

SDN Controller

Virtualized/Cloud Environment

Application

Malicious Application

Control Network

SDN Switch
Securing an SDN-based network

Protection of protocol interfaces (controller-switch i/f, possibly northbound i/f):
- preferably cryptographic protection (e.g. IPsec or TLS)
- sound, robust protocol implementations
- optionally a firewall in front of the controller to protect it against well known network and transport layer attacks (like TCP SYN floods)

Sound authentication and authorization concepts for network control by applications via the northbound interface, including conflict resolution

Security measures for virtualized/cloud environments when running the controller there (this is an issue of its own, to be solved independently of SDN)

Security measures as applicable also to traditional networks
Securing an SDN-based network – further details

**Security measures for virtualized/cloud environments**, like
- sound, robust implementations of the hypervisors and the overall cloud management software
- security zones (logical and optionally even physical separation/isolation)
- dedicated security functions (like firewalls) as part of the hypervisor or in VMs
- traffic separation (dedicated virtual switches, VLANs)
- cryptographic protection: traffic to/from/between VMs, data on storage

**Security measures as applicable also to traditional networks**, like
- secure OAM (Operation, Administration and Maintenance)
- secure operation of network protocols and services (e.g. routing, DNS, NTP)
- individual protection of each network function (formerly physical boxes, now VNFs)
Securing an SDN-based network

- Secure SDN controller
- Cryptographic protection
- Sound authentication and authorization concepts
- Robust implementation, overload control
- Cryptographic protection
- Robust implementation, overload control

Secure Virtualized/Cloud Environment

Application

Firewall

Control Network

SDN Switch

Public

© Nokia Solutions and Networks 2015
Using SDN to Improve Network Security

Advocates of SDN claim substantial benefits such as “Increased network reliability and security as a result of centralized and automated management of network devices, uniform policy enforcement, and fewer configuration errors” (from the ONF).

→ But network security will not increase by simply applying SDN!

Security opportunities do exist:
- **fine granular, agile control** over all traffic flows: monitor traffic on flow basis; block suspicious flows or redirect them to dedicated security devices
- **centralized control**: unify security policies, adapt them automatically and consistently
- **programmability**: implement security solutions as apps on the controller
- advantageous combination of SDN-based + traditional security solutions possible
- running controllers in cloud environments to make them resilient against DoS attacks
Straightforward example of an SDN-based security solution

Anti-DoS App policies

SDN Controller

Get Flow Statistics

Set Blocking Rules

Public SDN Switch

Target Server

Backup
Demo-setup: Mobile Guard interacting with de-composed gateways

Virtualized/Cloud Environment

S-GW App  P-GW App

GW control

Mobile Guard

Detect malware activity
Isolate infected terminal

Sanitizing Server

IP Service Network

Probe

S-GW U  P-GW U

Disclaimer: This is a demo setup, not an available Nokia solution!
SDN security products - examples

- Nokia’s Mobile Guard is a commercial security product - but SDN is currently only a “feature candidate”
- Radware Defense Flow (http://www.radware.com/Products/DefenseFlow/)
- HP SDN App Store (https://hpn.hpwsportal.com/catalog.html#/Home/Show)
  - HP Network Protector
  - Bluecat DNS Director
  - F5 BIG DDoS Umbrella
  - Guardicore Active Honeypot
- Related to network virtualisation: VMWare (NSX), Cisco (ACI) and others
## SDN security: Challenges versus opportunities

<table>
<thead>
<tr>
<th>SDN Feature</th>
<th>Challenge</th>
<th>Opportunity</th>
</tr>
</thead>
<tbody>
<tr>
<td>Separation forwarding/control</td>
<td>increased attack surface (but good protection mechanisms exist)</td>
<td>(basis for other opportunities)</td>
</tr>
<tr>
<td>Centralized control</td>
<td>successful attacks have huge impact</td>
<td>unify security policies, adapt them automatically &amp; consistently</td>
</tr>
<tr>
<td>Controllers in clouds</td>
<td>various threats, like attacks via hypervisor vulnerabilities</td>
<td>use elasticity of resources to overcome DoS attacks</td>
</tr>
<tr>
<td>Agile and fine granular control</td>
<td>increases complexity, is a source of errors, may be abused</td>
<td>facilitates security solutions that need to execute such control</td>
</tr>
<tr>
<td>Network programmability</td>
<td>abuse of control functions, exploiting vulnerabilities, compromising controllers</td>
<td>facilitates efficient deployment of security solutions running as applications on controllers</td>
</tr>
</tbody>
</table>
Conclusion

Security Challenges
Network programmability
Controllers in cloud environments

Security Opportunities
Unified but still agile control
Efficient deployment of security solutions as network applications

Considerable care and security awareness is required to mitigate the threats!

Turning the opportunities into better network security is a process that has just started!
**References**

<table>
<thead>
<tr>
<th>Reference</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>References</td>
<td></td>
</tr>
<tr>
<td>------------</td>
<td></td>
</tr>
</tbody>
</table>