Outsourcing Mobile Security in the Cloud

Gaëtan Hurel <gaetan.hurel@inria.fr>
Rémi Badonnel <remi.badonnel@loria.fr>
Abdelkader Lahmadi <abdelkader.lahmadi@loria.fr>
Olivier Festor <olivier.festor@inria.fr>

Plan

Introduction

Related work

Mobile Security as a Service

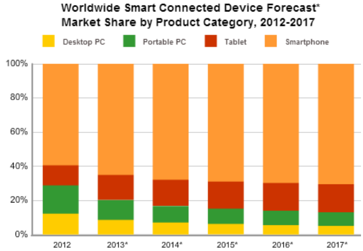
Preliminary results

Conclusions

Context

Ubiquity of mobile devices

- large-scale deployment
- mainly smartphones and tablets

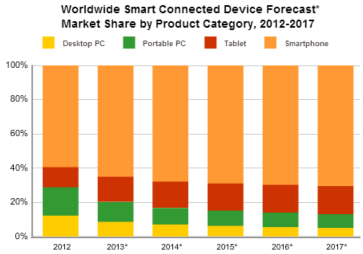


source: IDC analytics 2013

Context

Ubiquity of mobile devices

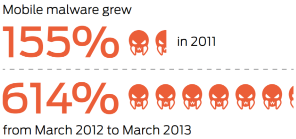
- large-scale deployment
- mainly smartphones and tablets



source: IDC analytics 2013

Mobile malware increase

- devices carry sensitive and valuable information
- numerous attacks & infection vectors


Mobile malware grew

155% in 2011

614% from March 2012 to March 2013

source: Juniper mobile threat report 2013

Traditional mobile security

On-device approaches:

- dedicated applications installed on the smartphones
- security checks mainly based on devices' resources

Traditional mobile security

On-device approaches:

- dedicated applications installed on the smartphones
- security checks mainly based on devices’ resources

Limits of on-device security approaches

- resource consumption
- installation, configuration & maintenance
- users’ awareness and involvement

Traditional mobile security

On-device approaches:

- dedicated applications installed on the smartphones
- security checks mainly based on devices' resources

Limits of on-device security approaches

- resource consumption
- installation, configuration & maintenance
- users' awareness and involvement

⟹ How to efficiently provide security for mobile devices using cloud-based mechanisms?

Plan

Introduction

Related work

Mobile Security as a Service

Preliminary results

Conclusions

Virtualization and cloning methods

Virtual replicas of real devices [1]

- execution traces and traffic mirroring from real devices
- real devices' activity replayed on replicas
- detecting threats on replicas, applying protections on devices

Virtual mobile instances (VMI) [2]

- with larger resources to host complex applications
- accessed by real devices to execute those applications
- dedicated monitoring subsystem to detect anomalies within VMIs

Mobile security functions outsourcing

Pure cloud-based outsourcing

- e.g. application firewall [3], antivirus [4]

SDN-based outsourcing [5]

- leverages network controller's global view
- security checks transparently applied on traffic

NFV-based outsourcing [6]

- dynamic deployment of middleboxes in the cloud using virtualization
- not dedicated to mobile security, but shows the potentiality of the cloud

Motivation

Limitations of current cloud-based approaches:

- focus on specific instance(s) of the whole security threats set
- lack of flexibility and contextualization regarding how and when to use them

Motivation

Limitations of current cloud-based approaches:

- focus on specific instance(s) of the whole security threats set
- lack of flexibility and contextualization regarding how and when to use them

Security threats may vary depending on context:

- time and space (e.g. malware trends, attached network)
- applications (e.g. gaming, banking)
- remote destinations (e.g. unknown/well-known server)

Motivation

Limitations of current cloud-based approaches:

- focus on specific instance(s) of the whole security threats set
- lack of flexibility and contextualization regarding how and when to use them

Security threats may vary depending on context:

- time and space (e.g. malware trends, attached network)
- applications (e.g. gaming, banking)
- remote destinations (e.g. unknown/well-known server)
- ...

Plan

Introduction

Related work

Mobile Security as a Service

Preliminary results

Conclusions

Proposed approach

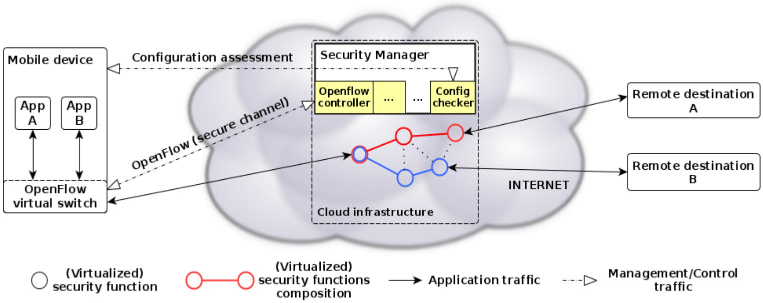
Dynamic composition of mobile security functions in the cloud:

- outsource mobile security functions in the cloud
- dynamically select and activate security functions
- transparently link and instantiate compositions of security functions

Main enablers:

- Network Function Virtualization (NFV)
- Software-Defined Networking (SDN/Openflow)

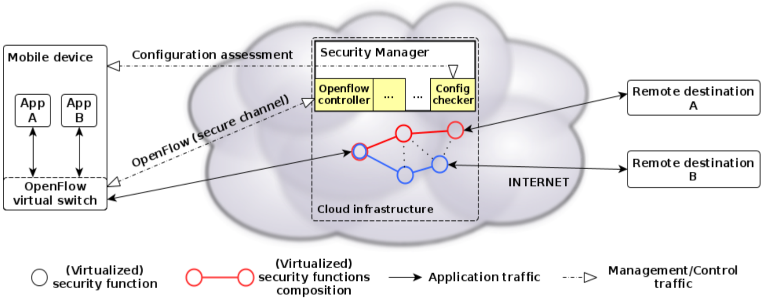
Our cloud-based mobile security architecture



A new cloud-based architecture to:

- host a large set of mobile security functions
- build and deploy tailored security compositions depending on context and risks

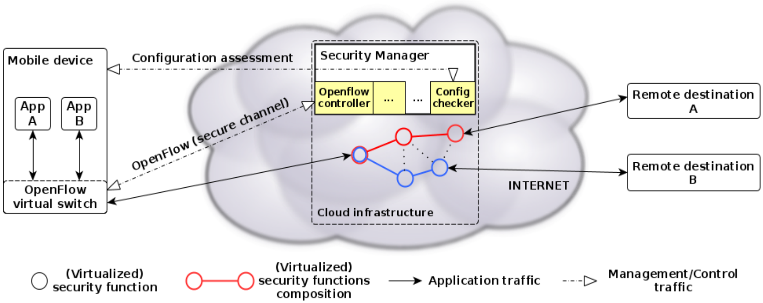
Key entities



Involves three entities:

- the mobile device with running applications and a virtual OpenFlow-based switch
- the security manager - in cloud infrastructure - to manage outsourced security functions
- the remote dest. interacting with the mobile device

Main idea



An application wants to communicate with a (new) dest. :

1. the switch probes the OpenFlow controller
2. the security manager possibly activates new security functions
3. the controller links those functions and build a tailored composition
4. the controller notifies the switch of the resulting composition
5. the switch makes traffic pass through the security composition

Plan

Introduction

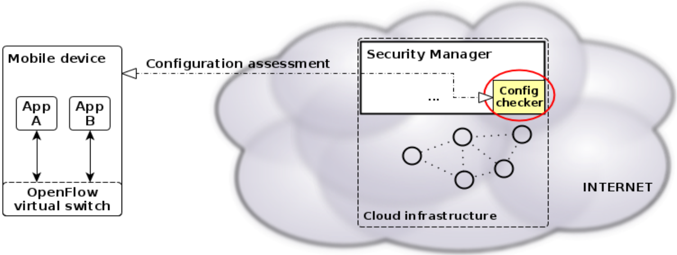
Related work

Mobile Security as a Service

Preliminary results

Conclusions

Our first outsourced security function



Implementation of a configuration checker for mobile devices [7].

Our first outsourced security function - cont'd

Outsourced configuration checker:

- based on the OVAL standard
- remotely checks configuration of mobile devices
- detects vulnerable states
- implements a probabilistic model to efficiently schedule assessments

Our first outsourced security function - cont’d

Outsourced configuration checker:

- based on the OVAL standard
- remotely checks configuration of mobile devices
- detects vulnerable states
- implements a probabilistic model to efficiently schedule assessments

⟶ Collected information about vulnerable configurations can be exploited by the security manager

Plan

Introduction

Related work

Mobile Security as a Service

Preliminary results

Conclusions

Summary

Mobile security is a critical issue

- mobile devices largely deployed
- numerous privacy and security issues
- on-device security approaches limits

Summary

Mobile security is a critical issue

- mobile devices largely deployed
- numerous privacy and security issues
- on-device security approaches limits

Cloud + NFV + SDN = efficient mobsec outsourcing

- reduction of devices’ resources usage
- dynamic security depending on context and risks
- transparent deployment from an end-user view

Future work

Mathematical modeling:

- investigate compositions mechanisms
- determination of cost (resources), quality and complexity of compositions
- tradeoffs between on-device and in-cloud security functions

Future work

Mathematical modeling:

- investigate compositions mechanisms
- determination of cost (resources), quality and complexity of compositions
- tradeoffs between on-device and in-cloud security functions

Prototyping and evaluation:

- OpenVSwitch deployed on Samsung Galaxy S4
- experiments with the Mininet simulator
- later: Openstack & NFV integration

Bibliography

[1] Portokalidis et al. Paranoid Android: Versatile Protection for Smartphones. *Proceedings of the 26th Annual Computer Security Applications Conference (ACSAC'10)*

[2] Kim et al. Monitoring and Detecting Abnormal Behavior in Mobile Cloud Infrastructure. *Proceedings of the 12th IEEE/IFIP Network Operations and Management Symposium (NOMS'12)*

[3] Kilinc et al. WallDroid: Cloud Assisted Virtualized Application Specific Firewalls for the Android OS. *Proceedings of the 11th IEEE International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom 2012)*

[4] Oberheide et al. Virtualized In-Cloud Security Services for Mobile Devices. *Proceedings of the 1st Workshop on Virtualization in Mobile Computing (MobiVirt'08)*

[5] Jin et al. Malware Detection for Mobile Devices Using Software-Defined Networking. *Proceedings of the 2nd GENI Research and Educational Experiment Workshop (GREE 2013)*

[6] Sherry et al. Making Middleboxes Someone else's Problem: Network Processing As a Cloud Service. *Proceedings of the ACM SIGCOMM 2012 Conference on Applications, Technologies, Architectures, and Protocols for Computer Communication*

[7] Barrere et al. A Probabilistic Cost-efficient Approach for Mobile Security Assessment. *Proceedings of the 9th IFIP/IEEE International Conference on Network and Service Management (CNSM'13)*