Implementing Secure Communications for Business-Use Smart Devices by Applying OpenFlow

SAIDA Yoshinori, IIHOSHI Takahiro, MORITA Gen, WATANABE Yoshikazu, KARINO Shuichi

Abstract

The increasing use of smart devices in enterprise businesses is making it an urgent task to take proper measures against information leaks. The NEC Cloud System Research Laboratories is conducting R&D into a flexible network control function that links networks and smart devices by introducing OpenFlow technology to smart devices. This paper introduces the improved safety of business communications using smart devices achieved by applying this technology.

Keywords

OpenFlow, Software-Defined Networking, BYOD (Bring Your Own Device), Virtual Private Network

1. Introduction

The use of smart devices such as smartphones and tablet terminals makes it possible to benefit from various business services through multiple wireless networks such as 3G, LTE (Long-Term Evolution) and Wi-Fi. Meanwhile, an important issue in the use of smart devices in business is how to ensure security.

This paper introduces a technology applying OpenFlow to secure the safety of business communications among smart devices.

2. Security Issues of Smart Devices

Smart devices adopt extended functions, as shown in **Table 1** , beyond those of traditional cell phones. These extensions make it possible to efficiently use various business services.

Table 1 Extended functions of smart devices.

Function	Advantage
Addition of downloaded applications	Introduction of business applications by enterprises
Wi-Fi	Use of high-speed Wi-Fi access points inside as well as outside the office
Tethering	Easy internet connection by connecting a PC
VPN (Virtual Private Network)	Use of an in-house network environment from outside the office
Large touchscreen panel	Smoother operation

Table 2 shows a classification of the security risks arising from these extended functions. The problems listed in this table require suitable countermeasures.

This paper introduces a technology applying OpenFlow to deal with these communications-related security risks. When storage-related risks are covered using another MDM (Mobile Device Management) solution, the combination will enable the safer use of smart devices in business.

3. Application of OpenFlow to Smart Device Communications Control

This section outlines the OpenFlow technology and its method of application to smart device communications control.

At the NEC Cloud System Research Laboratories, we are conducting research into a technology that applies OpenFlow for real-time control of the communications of smart devices on a network. [1)] This research aims to make smart device communications control more flexible according to the overall situation of the network and the requested services.

3.1 Outline of OpenFlow

OpenFlow is a network control technology with the following features. It enables flexible network management, operation control and adding new functions with software-based operations.

Implementing Secure Communications for Business-Use Smart Devices by Applying OpenFlow

Table 2 Risks caused by the extended functions of smart devices.

		Security risks			
		Illegal access	Impersonation	Reduced business efficiency	Increased operating costs
Function	Application addition	Information leak through malware infection	—	Use of non-business applications during business hours	—
	Wi-Fi	Bugging at vulnerable access points	—	—	—
	Tethering	—	Impersonated access from a non-permitted terminal using a permitted terminal as a stepping stone	—	Increased quantity of communications
	VPN	In-house system attack by malware		—	—

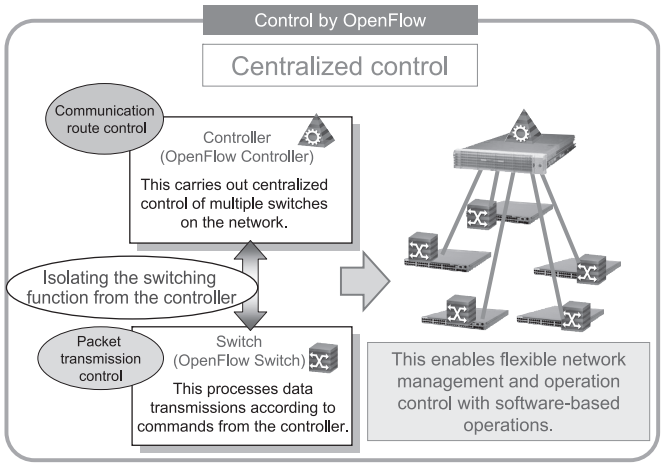

Fig. 1 OpenFlow concept.

(1) Centralized control

As shown in **Fig. 1** , an OpenFlow network is composed of an OpenFlow Controller (OFC), which controls the network route, and OpenFlow Switches (OFSes), which process packets according to the packet processing rules given by the OFC. It employs a "centralized control network" configuration in which the OFC installed in a network controls multiple OFSes.

(2) Fine granularity: per-flow control

OpenFlow manages communications according to a unit called a "flow," which is a combination of protocol information from the data link layer and the transport layer. As a result, it is capable of communications control with finer granularity than traditional communications control based on information from each layer of the OSI hierarchical model.

(3) Flexible software-based control

Traditional networks require dedicated equipment for network control, but OpenFlow can perform it by modifying the packet processing rules stored in the OFC. Together with the per-flow control described in (2) above, this feature makes possible flexible network management, operation control and adding new functions with software-based operations.

3.2 Application of OpenFlow to Smart Device Communications Control

At the NEC Cloud System Research Laboratories, we are advancing the research and prototyping of a system for controlling the communications of smart devices running OFS software from the OFC by applying OpenFlow technology to smart devices.

In this research, we assume two modes of application, which are shown as a) and b) in **Fig. 2** .

Comment a) in Fig. 2 shows the configuration in which the OFC is installed on the network and comment b) indicates the configuration in which the OFC is installed on each smart device. The OFS in the smart device is controlled by either OFC. In either configuration, incorporation of the OFS in the smart device makes it possible to identify the application communicating on the smart device from the information in the control unit called a "flow." The information obtained can be used for application-specific control, for example the selection of a wireless communications route such as 3G or Wi-Fi, and the denial of communication.

The difference in OFC installation location leads to the following difference in characteristics.

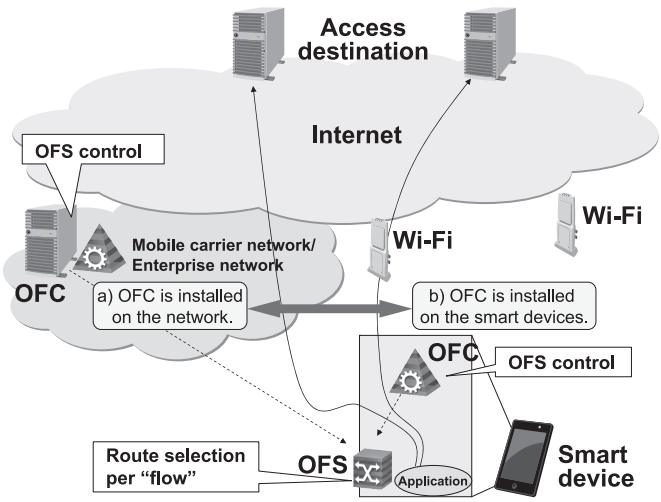

Fig. 2 Configuration of smart device communications control.

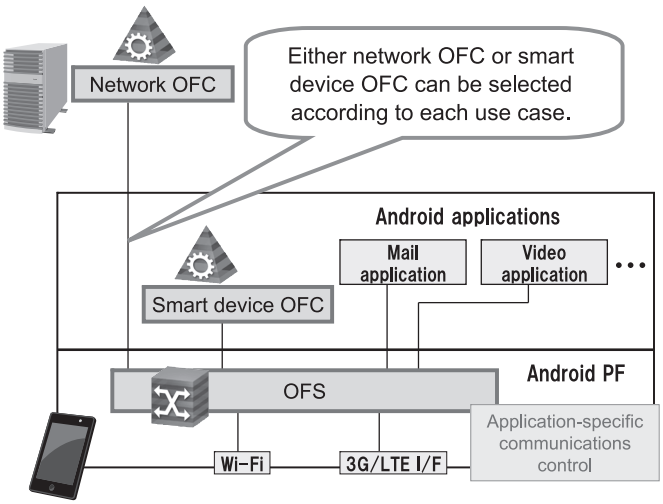

Fig. 3 Configuration of prototyping on an Android smartphone.

- **The OFC is installed on the network**
  When the OFC is installed on a mobile carrier network or enterprise network, centralized control of the communications of all the smart devices on the network is possible.
- **The OFC is installed on the smart device**
  The introduction of OpenFlow is facilitated because operations are possible with the smart device alone. However, additional linkage with an MDM system, etc. is required for centralized control of all smart devices.

At the NEC Cloud System Research Laboratories, we are currently advancing research and prototyping on the Android smartphone using the configuration shown in **Fig. 3** . As to the issue of network OFC and smart device OFC, either configuration can be selected to control the OFSes according to each use case.

4. Applications of Smart Devices in Improving the Safety of Business Communications

This section presents examples of applications of OpenFlow-based smart device communications control technology for improving the safety of communications by smart device business applications.

(1) Automatic communications network selection according to corporate policy
A business network can give instructions to smart devices to use 3G or Wi-Fi based on safety and cost of communications. With Wi-Fi, it is also possible to specify the Wi-Fi access point to connect to.

(2) Communications network selection according to application usage requirements
A communications network is selected automatically according to the requirements of the application running on the smartphone (communications safety, connectivity and bandwidth) and the user situation (inside or outside business hours, inside or outside the office and communication route).

(3) Automatic allocation of business communications to a VPN
It is possible to flexibly control the automatic allocation of VPN resources to business communications according to specific applications and access to specific sites.

(4) Blockage of malware communications
Notification to the user or blockage is possible for communications with a destination other than the server addresses specified in advance in a whitelist.

Fig. 4 shows the configuration of the system for implementing the control described above.

This system is composed of the OFC, which gives communications control instructions from the network to the smart device as described in section 3 above, and the OFS, which controls the communications of each smart device. These components implement the following functions.

Implementing Secure Communications for Business-Use Smart Devices by Applying OpenFlow

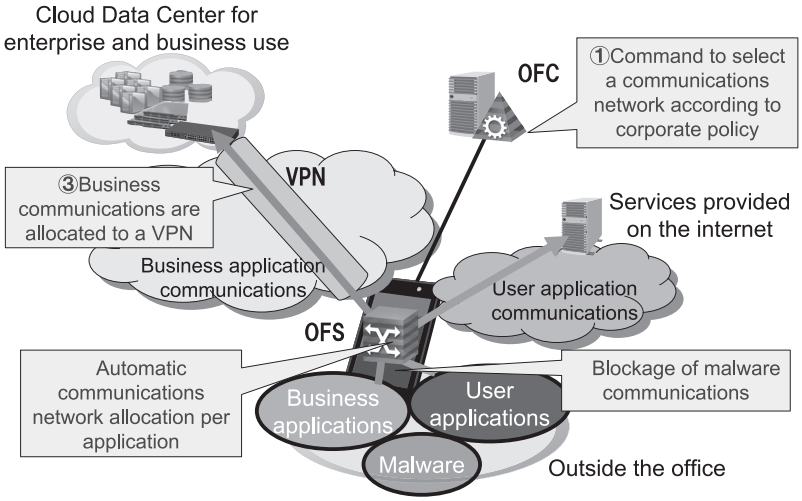

Fig. 4 Configuration of a business communications security improvement system.

- **Routing control per application and per communication destination**
  Based on instructions from the OFC, a wireless communications standard can be selected from among 3G, Wi-Fi and VPN for each application and each communication destination.
- **Detection and blockage of communications to an address not specified by the OFC**
  Communications conducted by malware running on a smart device with a destination other than the permitted addresses can be detected. Notification and detection information can be sent to the user or manager and the communication in question can be blocked.
- **Linkage with a smart device control application**
  An API (Application Programming Interface) for use in controlling the OFC from an application running on the smart device is provided to enable, for example, switching of communications control functions according to the context (location, time and usable networks) of the smart device.

These functions make it possible to provide safety for operations (1) to (4) above in the business communications of smart devices.

The biggest feature of this system is its ability to easily implement various functions related to communications control on a platform centered around an OFC and OFSes. New communications security risks can immediately be dealt with by simply adding new control software to the OFC installed on the network or smart device.

5. Conclusion

In the above, we introduced examples of a system for improving the business communications safety of smart devices by using a smart device communications control technology applying OpenFlow.

At the NEC Cloud System Research Laboratories, we are conducting R&D on the dynamic construction of a network offering optimum communications characteristics for each service based on the technology introduced herein. The results of this R&D will be used to create new services making full use of smart devices.

Part of the present research is conducted in the framework of “R&D of network virtualization infrastructure technology supporting new-generation networks” (topic A), a research subject commissioned by the National Institute of Information and Communications Technology (NICT).

*LTE is a registered trademark of European Telecommunications Standards Institute(ETSI).
*Wi-Fi is a registered trademark of Wi-Fi Alliance.
*OpenFlow is a trademark or registered trademark of Open Networking Foundation.
*Android is a trademark or registered trademark of Google Inc.

Reference

1) NEC Press Release, “NEC Develops Communication Control Technologies for Networks and Mobile Terminals to Reduce Transmission Overload,” 2011. 11
http://www.nec.co.jp/press/en/1111/0901.html

Authors' Profiles

SAIDA Yoshinori
Principal Researcher
Cloud System Research Laboratories
Central Research Laboratories

IIHOSHI Takahiro
Cloud System Research Laboratories
Central Research Laboratories

MORITA Gen
Cloud System Research Laboratories
Central Research Laboratories

WATANABE Yoshikazu
Assistant Manager
Cloud System Research Laboratories
Central Research Laboratories

KARINO Shuichi
Principal Researcher
Cloud System Research Laboratories
Central Research Laboratories

Information about the NEC Technical Journal

Thank you for reading the paper.
If you are interested in the NEC Technical Journal, you can also read other papers on our website.

Link to NEC Technical Journal website

Japanese

English

Vol.7 No.3 Smart Device Solutions

Vol.7 No.3
March, 2013

Special Issue TOP