Expert View

Security for your mobile apps: an inevitable requirement!

Christophe Brunet,
Product Manager – Mobile Security Solutions at equensWorldline

Christophe Brunet has worked as a Product Manager since June 2015. Previously he was the technical manager responsible for trust and security products, such as electronic signatures, secure archiving, and PKIs. And in this role, on several occasions he supported national and international certification processes (CSPN, RGS, Common Criteria, ETSI, PCI). He also worked on the online payment solution by Worldline: Sips.

In the first half of 2016
4 out of 5 infections *affected a smartphone*
compared with 1 out of 5 affecting a PC**

Mobiles: new hunting ground for fraudsters

For hundreds of millions of users worldwide, smartphones have become the way they access online services, particularly banking services. A study by Juniper* predicts that this number will double in the next three years to reach 2 billion. On average, a user of these online services connects to their bank **every day** from their smartphone, while they only go to their local branch twice a year. And this situation is currently being stimulated by the growth of digital banks.

Against this background, attempts of fraud and attacks are increasingly focused on smartphones, and many users simply do not know how to protect themselves. In the first half of 2016, 78% of software infections (see details below) were on smartphones, compared with 22% on PCs.**

Manifold threats of which users are unaware

Security threats on mobiles operate invisibly, in such a way that the user is usually completely unaware of them. The main aim of these attacks is to steal the information stored on the smartphone to then use it fraudulently. They can be classified as follows:

- **Malicious code:** spam, fraudulent links, misleading ads, compromised websites, and even SMS or MMS, are all ways to install malicious code on a smartphone.
- **Attacks on the mobile:** use of vulnerabilities on smartphones, their operating system, and the software installed, in order to take control of all or part of the device.
- **Physical access to the phone:** taking advantage of a moment's inattention from the device owner, the fraudster physically gets hold of the phone to install malicious software on it or directly access data.
- **Interception of communication:** mobiles are highly sophisticated devices that communicate over several channels (data networks, Wi-Fi, Bluetooth, NFC). Interception technologies are available on these networks and allow "man-in-the-middle" attacks to take place.

**October 2016 – Juniper is an analyst firm in the mobile and digital tech sector.*

***source Nokia Threat Intelligence report H1 2016*

Worldline

Security for your mobile apps: an inevitable requirement!

The risky behavior of smartphone users who are unaware of these problems amplifies the risks of attacks. Some examples include:

- **Rooting or jailbreaking cell phones:** This fairly widespread practice removes the access protections on administration actions for the device, making it easier for external parties to enter the core operation of the device.
- **Failure to update cell phones:** The operating systems and installed apps often have vulnerabilities that fraudsters know how to exploit. Regularly updating all of the cell phone's software limits the potential gaps through which fraudsters attack.
- **Unofficial apps:** Suppliers of operating systems offer apps that they have checked and certified in their stores. This limits the risk of viruses and malware. However, if you download an app from an unofficial source there are generally no security guarantees.

Putting in place a real security policy in smartphones for your mobile apps

While there might be no such thing as zero risk, it is possible to create a checked and controlled high-trust environment for your mobile apps directly on users' smartphones.

To do so, you need to implement a security policy on the smartphone that can be adapted as the strategies of fraudsters evolve. It is based on three key functions: detection, analysis, and decision.

First, you need to be able to **detect** characteristic markers of potential risks or weaknesses that are threatening the security of the cell phone, installed apps, and the data stored. This detection is based on the activation of sensors integrated into the app. These sensors collect information on the security level of the cell phone (app and OS versions, existence of an emulator or debugger, connection profile for an app, etc.).

This information must then be **analyzed** and evaluated in relation to the security policy defined by the developer.

From this evaluation, the app can then **decide** to provide its service in full or in part by limiting or prohibiting certain functions.

Strengthening the security on the smartphone in this way will reduce the risk of fraud, improve user trust, and increase the adoption rate of mobile services.

With several decades' experience in securing sensitive electronic transactions, Worldline is now putting its expertise to use with mobile transactional services by launching its WL Mobile Intrusion Protection solution.

Available for Android and iOS and complying with the European regulations on the protection of personal data, **WL Mobile Intrusion Protection** relies on a large range of sensors that can be used as desired, and directly configurable security policies for each cell phone.

This self-adapting solution also supplies a centralized system with data collected anonymously on each device, so as to repeatedly fine-tune the security policies: detection, evaluation of risks and decision on the service level provided. These policies are then redeployed on smartphones when they next go online.

About Worldline

Worldline [Euronext: WLN] is the European leader in the payment and transactional services industry. With innovation at the core of its DNA, Worldline's core offerings include pan-European and domestic Commercial Acquiring for physical or online businesses, secured payment transaction processing for banks and financial institutions, as well as transactional services in e-Ticketing and for local and central public agencies. Thanks to a presence in 30+ countries, Worldline is the payment partner of choice for merchants, banks, public transport operators, government agencies and industrial companies, delivering cutting-edge digital services. Worldline's activities are organized around three axes: Merchant Services, Financial Services including equensWorldline and Mobility & e-Transactional Services. Worldline employs circa 11,000 people worldwide, with estimated pro forma revenue of circa 2.3 billion euros on a yearly basis.

For further information
infoWL@worldline.com