BYOD: Security and Privacy Issues in 4 Smartphone Platforms

EraldaCaushaj, Ivan Ivanov
{eralda.caushaj, ivan.ivanov}@esc.edu
Huirong Fu, IshwarSethi
{fu, isethi}@oakland.edu

Abstract

Many corporates are implementing bring-your-own-devices (BYODs) policy in nowadays. Accessing company's data on personal devices along with increased productivity and efficiency raise a lot of privacy and security concerns. Based on the data captured by conducting real-life scenarios in four different platforms such as IPhone, Android, Windows, and Blackberry we realized that various useful apps installed and used by the end-users have serious issues in terms of privacy and the information exposed. The focus of our paper is to study the storage and intercommunication features and compare the four platforms in terms of limitations and how they handle the division of personal and work apps and data in a smartphone. What is the better platform in terms of privacy and what restrictions and policies should be applied by the corporates to better implement the BYOD policy?

Introduction – Mobilityand BYOD Initiatives

The prediction and trend from the surveys conducted by Microsoft with customers show that by 2014 mobile internet should take over desktop internet usage. Statistics show that there are over 1.08 billion Smartphone users in the world today and 91.4 million of them are the U.S [1]. The market share of the smartphone platforms in 2011 was divided as detailed in Figure 1. Android had the largest market share than any other platform with 46.9 percent and Symbian the lowest one with 1.5 percent. Since the market share of the Symbian platform is too low compared to the other ones we consider for security and privacy attacks just four platforms as follows: IPhone, Android, Windows, and Blackberry.

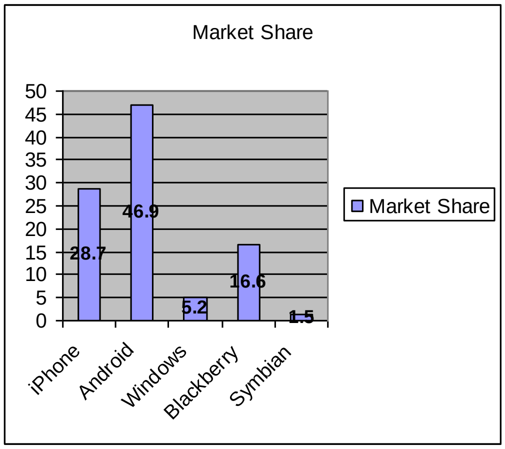

Figure 1. The market share of the five platforms used by smartphone users in 2011

BYOD is a growing trend in the private and public sector that allows employees the convenience of logging into the corporate network with their own personal devices. The raise of the mobile workforce to 1.2 billion in 2013, representing 35% of the worldwide workforce according to IDC

Forecast [2] drives forcefully the BYOD initiative as many of those workers will be using their own devices. While BYOD offers flexibility and efficiencies, the initiative brings a significant advantage to productivity as the quarterly Mobile Workforce Report from IPass Company found that many employees are working up to 20 additional hours unpaid as a result of company's BYOD policy [3]. However as with many advantages, there are a number of adjustments adopting organizations should consider when allowing personal mobile devices access to sensitive proprietary information.

BYOD-Security and Privacy Challenges

A substantial hindrance for IT departments is how effectively to manage the corporate network access and to secure application and data content for user-owned devices. Some of the major BYOD challenges are listed as follows [4]:

- Personal-use restrictions: A personal device can be used for work purposes, but the apps installed and used might interfere in terms of privacy with the sensitive documents and work purposes emails. The policy should make clear what users can and cannot do with the device.
- Access: The policy should clarify the corporate's access to the device; for instance, to install a security app that creates a "sandbox" for government apps within the devices memory.
- Security: The corporate must be able to remotely wipe the device in the event of loss such as personal apps, photos and such would be lost).
- Data ownership: The policy should set procedures for retrieving the government's data when the officer leaves, or changes agencies or jobs.
- The phone number ownership: The policy should deal with the issue when employees leave the company if they should take their phone number with them or not.

The applications are one of the major privacy risks in smartphones. IBM propose two efficient methods how to prevent vulnerabilities in mobile applications [5]:

- Best practices for writing application code
- Detect attacks using taint analysis: Taint analysis is a specific type of static analysis that detects integrity violations, such as applications using data from untrusted users. It is also helpful to identify confidentiality leaks, such as applications using private user data.

Mobile Platform Architecture Overview

Researchers at Oakland University conducted experiments in four different platforms such as Iphone, Android, Windows and Blackberry. The packets captured through Wireshark for approximately 24 minutes, gave significant information regarding security and privacy issues involving the users. A lot of useful apps installed and used by the end-users have serious issues in terms of privacy and the information exposed [6]. Our focus will be to analyze, identify and compare the privacy risks in each platform, based on the operating system's features that the major smartphone companies are using.

A. IOS

Security risks: iOS applications can expose confidential data when communicating with a web server, opening web views or creating external notifications [5].

Privacy performance metrics:

a. Storage
b. Intercommunication of apps with OS

B. Android

Security risks: Popular Android applications can leak data when connected to a vulnerable network, such as a Wi-Fi hotspot. This means someone on the network could modify the content in transit. In addition, opening web views with native Android applications can introduce common web security issues, such as cross-site scripting attacks via JavaScript. Loading code from external storage devices can also create security exposures such as another application could modify the content on the device [5].

Privacy performance metrics:

a. Storage
b. Intercommunication of apps with OS

C. Blackberry

Privacy performance metrics:

a. Storage
b. Intercommunication of apps with OS

D. Windows Smartphone

Privacy performance metrics:

a. Storage
b. Intercommunication of apps with OS

Buildinga BYOD Strategy – A Decision Framework

The serious challenges in developing BYOD strategy and the consecutive framework for its implementation is the impact BYOD can have on individuals' privacy, organizational security, and the liability of the both entities. The Gartner analysts Andy and Nick Jones in their Checklist for Determining Enterprise Readiness to Support Employee-Owned Devices [9] have analyzed and defined a structured approach in seven phases on the road to this emerging trend driven by consumerization of IT.

For corporate IT structures and embraced BYOD framework we consider the following key steps encapsulate in:

- Reasoning and deciding on a BYOD strategy – identify corporate mobile needs, define BYOD scope, shape sponsors' and stakeholders' commitments and responses to a BYOD program
- Design BYOD program segmentation by roles/needs/functions in the organization – categorize internal and external support, the range and type of access, and create packages of Policies and Technologies for each group
- Plan BYOD implementation by streamlining tools and technologies, network infrastructure and services, financing models, and exit options such as:
    - classify and approve list of devices and versions of mobile operating systems, applications, and providers;

  - design uniform policies, to enable scalable control and management of the user-owned mobile device utilizing Mobile Device Management (MDM), Mobile Applications Management (MAM), and Mobile Content / Document Management (MCM) solutions;
  - acceptable use policy with user's responsibilities and organization's rights against user's possession;
  - reimbursement plan options, total cost of ownership, corporate / private ownership separation and list of approved exit options.
- Program setup and approval – complete internal policy, procedures, contracts, agreements, and training documents, educate stakeholders and ensure their sign-off, gain sponsors budget and program approval
- Perform proof of concept by running a pilot over selected BYOD segmentations - modify procedure / policy / technologies based on the feedback and lessons learned from the pilot
- Program execution and evolution – periodic review and update of the BYOD program with current software versions, devices, applications, and providers.

The early BYOD adoptions have already experienced numerous concerns regarding losing personal data and privacy as corporations took full control over personal devices, applications, and information by utilizing mobile device management and device-level layer 3 VPNs. To address most of those critical anxieties instead of a full control of the personal device, most corporations currently focus on adopting a set of tools to enable IT departments to wrap corporate applications in a security layer and to make sure that the enterprise control on the personally owned device is limited only to the corporate data and applications. This actually shifts from Mobile Device Management to Mobile Application Management and from device-level VPNs to explicit application-specific VPNs involving technologies such as BIG-IP APM AppTunnels and encrypted connection to specific service supported by Microsoft Exchange [10].

Assessingand Evolving BYOD Program

Based on the research illustrated in Section III and on the Framework outlined in the previous section we are planning a multidimensional approach for assessing the critical phases of BYOD policy implementation:

- Risk Analysis – Validate the strength of the BYOD policy from at least four key factors:
  - *Social* (Costumers and Employees Satisfaction)
  - *Operational* (Business Process Continuity and Evolution)
  - *Financial* (Forming Business Metrics over the lifecycle of the BYOD program)
  - *Technical* (Risk Avoidances and Risk Management– how to prevent mobile security threats, how to handle disastrous events).
- Legal Issues and Privacy Concerns - all possible scenarios should be covered in the BYOD contracts / agreements signed off by both sites - the company's authorities and all mobile users. The most common cases in the service contracts address actions such as:
  - when mobile user utilize personal smartphone for personal and work purposes, the company owns the right to wipe out the corporate documents from the user's device in case of lost or hacked. The personal information should be guaranteed not to be erased or modified by the company's reaction.

- The company owns the device when it is totally used for work purposes. All information in that devise can be erased or modified anytime according corporate rules and regulations.

The current generation of mobile users demand a high quality wireless experience all of the time. Mobile workers depend on it and when it is not delivered as expected productivity drops ultimately costing company productivity, profits, and brand reputation. Therefore the quality of user experience needs to be at the heart of any BYOD Strategy. The adopted corporate framework has to provide consistent, predictable, frequently updated, and secure experience for all users of the utilized mobile platforms, devices, and/or applications.

Bibliography

[1] Richmond, H., “Microsoft Tag. In The Growth of Mobile Marketing and Tagging,” Retrieved July 13, 2012, from: http://tag.microsoft.com/community/blog/t/the_growth_of_mobile_marketing_and_tagging.aspx.
[2] International Data Corporation (IDC), Worldwide Mobile Worker Population 2009-2013 Forecast and Worldwide Mobile Enterprise Management Software 2012-2016 Forecast and Analysis and 2011 Vendor Shares, Sept., 2012, Retrieved on June 28, 2013 from: http://www.gotomypc.com/remote_access/images/pdf/How_to_Equip_Your_Company_for_the_New_Mobile_Workforce.pdf
[3] ComputerworldUK, BYOD Makes Employees Work Extra 20 Hours Unpaid, August, 2012, Retrieved on July 1, 2013 from: http://www.computerworlduk.com/news/mobile-wireless/3377143/byod-makes-employees-work-extra-20-hours-unpaid/
[4] CDW, "Mobile Strategies For Government," Retrieved on July 2, 2013 from http://webobjects.cdw.com/webobjects/media/pdf/Solutions/mobility/CDWG-Mobile-Devices.pdf?cm_re=WaysToShop-_-Mobility-_-Mobile+Strategies+for+Govt
[5] IBM Software, March 2013, "Ensuring application security in mobile device environments," Retrieved on July 2, 2013 from http://www.ndm.net/mobile/pdf/WGW03009USEN.PDF
[6] Caushaj, E., Fu, H., Sethi, I., Badih, H., Watson, D., Zhu, Y., Leng, S.,"Theoretical Analysis and Experimental Study: Monitoring Data Privacy in Smartphone Communications," IJITN 2013.
[7] White House, A Toolkit to Support Federal Agencies Implementing Bring Your Own Device (BYOD) Programs, 2012, Retrieved on June 28, 2013 from: http://www.whitehouse.gov/digitalgov/bring-your-own-device
[8] SouppayaMurugiah, and Scarfone Karen, NIST Special Publication 800-124, Guidelines for Managing the Security of Mobile Devices in the Enterprise, 2013, retrieved on June 27, 2013 from: http://www.nist.gov/manuscript-publication-search.cfm?pub_id=913427
[9] Rowsell-Jones, Andy, Jones, Nick, Checklist for Determining Enterprise Readiness to Support Employee-Owned Devices, Gartner, June 18, 2012, ID: G000234127
[10] Silva, Peter “BYOD 2.0: Moving Beyond MDM”F5 White Paper, Retrieved on 09/20/2013 from: http://www.f5.com/pdf/white-papers/big-ip-apm-mobile-application-manager-white-paper.pdf