A bird's eye view on Bring Your Own Device

Mattia Zago
Universidad de Murcia
mattia.zago@um.es

….

Abstract- **Este documento constituye la plantilla para las *II Jornadas Nacionales de Investigación en Ciberseguridad* (JNIC 2016), organizadas por el grupo *UCyS* de la Universidad de Granada (UGR). El *abstract* debe contener entre 100 y 150 palabras. El tipo de letra es *Times New Roman negrita, 9 ptos.*, tal y como aparece en esta plantilla. Se recomienda no emplear acrónimos en esta sección. Esta plantilla ha sido generada tomando como base el estándar de documentos IEEE. Por favor, utilice esta plantilla como formato base para su trabajo. Cualquier cuestión sobre el envío de las contribuciones debe dirigirse a la dirección electrónica jnic2016@ugr.es. Para más información sobre la organización y desarrollo de las jornadas, consulte el enlace http://ucys.ugr.es/jnic2016.**

Sigificant concerns about security (corporate have more to lose) and privacy (employees have more to lose).

***Index Terms*- BYOD, Bring Your Own Device, Mobile Device, Challenges, Environment Isolation, Mobile Management**

Tipo de contribución: *Investigación publicada / Investigación en desarrollo / Formación innovación / Formación talleres / Reto industria*

I. Introduction

"Anytime and everywhere" is the today's mantra. People are always connected and they are bringing personal devices at any place, including during work hours. This phenomenon takes the name of Bring Your Own Device (BYOD), and many organizations are confused (or at least concerned) about that.

Theorized in 2003, BYOD describes the "circumstances in which users make their personal devices available for company use" [1] and since 2011 it is not anymore an option: BYOD policies must be defined and the related issues must be faced.

A personal device is by definition "*a device that has not been configured and locked down by the company IT department*" [3], in fact, according to big multinational companies such as CISCO [4], OVUM [5] and TrendMicro [6], nowadays 95% of the employees are carrying and using their owned mobile phone at work. According to their survey, the average employee has at least 2.8 total devices including laptops, smartphones and tablets.

A. Benefits

Companies that allow BYOD seem more accommodating to employee's needs, and therefore a preferred place to work with a higher morale, resulting in a generic increase in the work efficiency. Not all the authors agreed with this productivity efficiency, indeed this situation is gradually degrading the boundaries between work-time and personal-time, leading to an ephemeral distinction between the twos. The fact is that most companies will fail in halt or obstruct BYOD phenomena, making the BYOD acceptance policies the only reasonable way to deal with personal devices. These policies must be more sophisticated and feasible, permitting the definition of multiple scenarios both in abstract and in concrete situation: which devices are allowed/safe/acceptable? Which OS versions can be considered secure? Which are the minimum enforce rules that must be applied to each device? Which kind of applications will be permitted? How the company networks will change? Which subnetworks will be available to which devices?

BYOD can be seen as a cost-saving solution for enterprises, but at the same time cheaper IT infrastructures face higher risk in confidentiality, integrity and availability of corporate data.
According to TrendMicro, the key factors that are driving companies to deploy BYOD programs are the aforementioned employees increased productivity and the improved employee flexibility (in terms of access to corporate data, chosen device and competitive differentiation).

II. Challenges

BYOD scenario changes the perspective about the IT security treats. Along with the classical Confidentiality, Integrity and Availability challenges (CIA, such as application security, data and device protection, information control, etc.) the introduction of the mobility paradigm substantially increase the risk factor of several threats, including data manipulation, data leaks and denial of services. It is possible to remap these issues in two macro challenges: Environment Isolation and Mobility Management.
Environment isolation refers to all the concept bound to the separation between corporate and personal environments (like virtualization, encryption, access control, information flow, etc.), while the mobility management refers to all the challenges related to the mobile hardware and software diversification (such as IT support, mobile network monitoring, patch delivery, policy enforcement, etc.).

A. Isolation

BYOD intuitively leads to the idea of separating personal data from corporate data. This can be achieved through different concepts, most of them are based on the hint of virtualized environment.
The virtualization concept is built on the idea of a middleware that permits to separate the operative system and the running software. This is accomplished usually through two distinct methods: virtualization and sandboxes. Virtualization is built on the trust given to the operative system, while the sandbox rest on the distrust of non-certified applications.
Independently from the chosen approach, isolation implies that all the issues related to authentication, availability and integrity were solved. For example, each data stored in the device must be encrypted, and therefore accessible only to an authenticated user; moreover, these data must be protected by some kind of

anti-tampering techniques such as signatures or remote validation.
In BYOD the isolation requirement must take in account the limited resources available and the highly-dynamic environment. The classic virtualization approach (full virtualization, para virtualization, resource virtualization) may need a structural review in order to be able to achieve important security properties in a BYOD scenario: e.g. shifting from session virtualization to a native application specifically designed for mobile OSs.

B. Mobile Management

While isolation underline a group of technical issues, mobile management is a set of design-level challenges, such as definitions of regulatory policies and frameworks, device management models and risk models. For example, the old-fashioned scalability property doesn't impact mobile applications requirements since each of them lives inside a very limited, fixed and well-defined resource boundary.
At design level many questions must find an answer, such as: when, and in what situations, an employee is acting as a corporate representative? Which is the boundary between private data and corporate data (including sensors data)?
Generally, enterprises need to define the employees' rights in terms of privacy and devices usage, especially when devices are not owned by the IT department (under the assumption of the fact that when data migrate to a personal device they are no longer under control).
This can be achieved through policies that outline explicitly minimum requirements (from physical device protection to patch and updates installation) and express the organization awareness about the risks. Several changes are required in order to include mobiles devices into risk models, and since a compromised device can move between different areas of the network they can bypass border controls (connecting to a wired network can place the device inside the corporate intranet, behind the boundary firewalls). Therefore, several physical requirements may be enforced and extent to mobile devices, for example force to turn off wireless connections in sensitive facilities, forbid to take photos or audio, etc. Further researches are required to develop or improve enterprise-specific policies and regulatory frameworks from the existing information security standards and user compliance methods.
Moreover, enterprises, and organizations in general, must define and apply a device control framework that permits to deploy security and behavior policies.
In literature there exists several examples of such frameworks, in general they are offering support to companies in terms of resources and services availability, such as management of policy, security features, inventory and software distribution.
All of these frameworks can be categorized in three groups: Mobile Device Management (MDM), Mobile Application Management (MAM), and Mobile Information Management (MIM), where:

- MDM remotely monitor and control the devices, offering a full control over both personal and corporate data locally stored, with the objective of securely manage both information flow and administrative operations. Is useful for small and medium enterprises that needs to deploy BYOD strategies rapidly with a centralized solution;
- MAM, provides application support, such as provisioning, remote configuration, updates and backups. Corporate apps can be locked, restricted or remotely updated, while user's applications - outside the MAM boundaries - are then considered private as long as their working principles are not in conflict with corporate applications;
- MIM, goes beyond the limitations of MDM and MAM (which are limited by the poor user experience) by removing all the limitations in terms of installable applications and permitted devices, but restricting the access to corporate resources (such as private cloud) by allowing a limited number of trusted applications to control and manage them.

Neither MDM, MAM nor MIM are complete solutions, and all of them suffers of several issues: MDM is controversial, because usually users feels restricted and because a poorly estimate risk can still leave the phone unprotected if stolen or lost. On the other hand, MAM and MIM are dual because MAM ensure some application security properties but does not explicitly protect data, while MIM's focus on data integrity and encryption provide only a minimum protection against malware, tampering or data synchronization.

III. CONCLUSIONS

Clearly there are several important advantages for employees and employers when employees bring their own device to work.

The security models around BYOD summarized in two opposite approaches: hands-off devices vs hands-on devices.
The former is really effective when the services are delivered according to the desktop virtualization/application style. The latter approach is based on a tight control, manage and monitor of data, applications, settings and network usage.

BYOD threats are sophisticated and require a layered security strategy that minimize the risk while maintains the compliance with the laws. This require a shift from protecting the devices to protecting the corporate data in terms of compartmentalization of information, better audit process and more incisive BYOD strategies.

In general, each BYOD scenario must be defined with particular attention to estimated costs, risks, and information security response. Moreover, the adoption of any BYOD solution should be simple and friendly, where security constraints are enforced differently considering the kind of roles, tasks and user reputation.

This is a particularly complex area for organizations and need to be researched, as it involves cross-disciplinary comparative assessments of benefits and risks, where neither organization-wide benefits nor a complete empirically based picture of information security threats are yet available.

It's evident that BYOD security requires further research and development.
Existing frameworks must become flexible tools that perfectly suit specific business needs.

Our future work will focus on those two macro areas
Risk + mobile + malware spread + design view + prototype

IV. REFERENCES

[1] G. Disterer and C. Kleiner, "BYOD Bring Your Own Device," *Procedia Technology*, vol. 9, pp. 43-53, 2013.

[2] N. Leavitt, "Today's mobile security requires a new approach.," *Computer*, no. 11, pp. 16-19, 2013.

[3] S. Mansfield-Devine, "Interview: BYOD and the enterprise network," *Computer Fraud & Security*, vol. 2012, no. 4, pp. 14-17, 2012.

[4] J. Bradley, J. Loucks, J. Macaulay, R. Medcalf and L. Buckalew, "BYOD: A Global Perspective Harnessing Employee-Led Innovation," CISCO IBSG Horizons, 2012.

[5] Logicalis, "BYOD: an emerging market trend in more ways than one," OVUM, 2012.

[6] Forrester Research, INC, "Key Strategies To Capture And Measure The Value Of Consumerization Of IT," Trend Micro, 2012.