BYOD and mobile security over a coffee

Business Services

orange™

editorial

Mobile phones and tablets have become both professional tools and status symbols. As more and more of us carry these must-have devices wherever we go, their security has emerged as a major challenge to both manufacturers and traditional security developers.

So in a developing, diverse market that isn't (yet) immune to unexpected disaster, what challenges does a Bring Your Own Device (BYOD) culture have in store for companies? What exactly is at risk when you lose your phone? And, lastly, what security devices can combine personal and professional use? These are some of the questions we will try to answer during this coffee break!

We hope you enjoy reading this, and we'll see you soon on our blogs!

Philippe Macia

content

in search of... lost smartphones

by Vincent Maurin

What happens when a smartphone without a security system is left in the middle of an urban jungle? Experts from Symantec have tried to answer this question with the "Smartphone Honey Stick" project.

the honey pot

In cooperation with Perspective Inc., Symantec researchers had the (bad?) idea of **"losing" 50 smartphones** in the middle of five major North American cities: New York, Washington DC, Los Angeles, San Francisco and Ottawa. Abandoned in busy public spaces, the 50 smartphones contained **applications that tracked their location and use**.

Since smartphones hold valuable personal and professional information, the Symantec researchers were interested to see how people who stumbled across the devices would behave.

"lost" smartphones

The 50 smartphones had no security system (password, etc). As stated in "The Symantec Smartphone Honey Stick Project", the study aimed to analyze "human threats" to phones. It was designed to determine the probability that the finder of a device would:

- unlock the phone (and the time it would take to do so)
- access professional data and applications
- access personal data and applications
- access applications depending on type

• return the smartphone to its owner
• take the smartphone with him/her (and the time it would take to do so)

The researchers assumed that the finder would access the phone's data or applications for one of the following reasons:
• identifying or locating the owner to return the device
• reading content for curiosity's sake
• researching valuable information
• using it personally (calls, Internet access)
• resetting the phone for resale or reuse

rigged applications and data

Every smartphone had a set of improperly functioning applications with easy-to-understand names and icons. In some cases, applications simulated a malfunction by sending an error message to the user:

app type	information category
social networking	personal
online banking	personal
webmail	personal
private pix	personal
passwords	neutral
calendar	neutral
contacts	neutral
cloud-based docs	neutral
HR cases (PDF)	corporate
HR salaries (spreadsheet)	corporate
corporate email	corporate
remote admin	corporate

Source : Symantec Smartphone Honey Stick Project

“sensitive data was the primary goal”

warning

The purpose of these applications was to collect data on user activity and communication. A GPS tracking device was also implemented **to track the smartphone's movements.**

Certain applications asked the user to enter a password, but then authenticated the user with a pre-filled code. The list of contacts was short and included a "Me" entry, making it easy to identify the phone's owner.

interesting results ?

When looking at the results of the Symantec study, we must keep in mind that **the sample size was small** (only 50 phones). We also need to remember that little is known about the specific characteristics of the various urban environments (number of passers-by, layout, time of day, etc).

For those who are too impatient to read the full study, here is a summary of the results.

People who found the smartphones:
• unlocked the device in 96% of cases
• accessed personal data and applications in 89% of cases
• **accessed business data and applications in 83% of cases**
• accessed both personal and professional data and applications in 70% of cases
• contacted the owner in 50% of cases

good to know
People accessed business data and applications in 83% of cases.

Viewing sensitive data was the primary goal of many people who found phones:
• they attempted to **open the professional email inbox in 45% of cases**
• they opened data marked "human resources" under "salaries" in 53% of cases and under "files" 40% of cases

• they opened **“remote administration” application in 49% of cases**

Curiosity was obviously a motivating factor:
• data or at least one application was opened in 96% of cases
• **personal photos** were opened in **72% of cases**
• **banking applications** were opened in **43% of cases**
• **personal accounts** (social media, messaging) were opened in **60% of cases**
• **the “passwords” file** was opened in **57% of cases**

Since 50% of smartphones were returned to their users, the results can be interpreted positively (as Symantec researchers did) or negatively**.**

recommendations

What can we learn from this study? Not much, except how important it is **to take measures to protect your personal and professional information** (e.g., passwords).

original article
http://oran.ge/13lkX9p

don’t touch my BOYD!

by Jean-François Audenard

Using your **personal equipment** (iPhone, iPad, and Android and other mobile devices) for professional purposes has almost become the new norm. The BYOD phenomenon is the result of a groundswell movement. Companies are now torn between the advantages of this model and the **security challenges** it presents. At the same time, device owners have to stay vigilant and not let overzealous companies and technologies push them around.

technologically advanced

More and more people are using their **personal devices at the workplace**. Using their own devices lets them keep working while traveling, commuting or staying home. One of the reasons behind this movement is that very often (too often?) these devices are **more powerful and user-friendly** than the “antiques” their company provides them at work.

companies at a crossroads

Companies are dreading the consequences of BYOD, which can lead to leaked data or unauthorized access. Cutting to the chase, can BYOD pose a big enough threat to be banned from companies? No.

On the contrary, **BYOD is a golden opportunity** for companies for two reasons:

1. it **reduces IT costs** because employees buy their devices themselves
2. it **increases employee productivity**. It helps pick up a few

precious extra hours of work without having to pay for them, or for additional labor costs.

It's not just the "in" thing to do: allowing and encouraging BYOD provides a business advantage for companies, as they look for ways to optimize costs in a difficult economic environment. For more analysis of this phenomenon and its challenges, check out my colleague Stewart Baines' article, "Why do we bring our own devices to work?"

read Stewart's blog post

BOYD security: a tough challenge!

Securing BYOD terminals is no easy task: as opposed to the devices they provide, **companies cannot dictate terms of use** and required security measures for devices owned by employees.

companies no longer make the decisions

Yep, it's a rule: for all employee devices, companies will have to get employees to agree before changing settings, installing security solutions, or even remotely geolocating or deleting data on the device.

To an extent, **employees can now take back control**, because they will only accept solutions that benefit them personally and professionally. And yes, IT and security managers will have to take employee expectations into account during negotiations.

“companies can no longer dictate terms of use and required security measures for devices owned by employees”

warning

VDI: the ultimate solution for BYOD?

But does securing a BYOD device solve the problem? Maybe there's another solution. Virtual Desktop Interface (VDI) technologies such as Citrix (XenDesktop ou XenApp) and VMware (VMware View) now make it possible to remotely access company applications from nearly any kind of device.

good to know

Not only does BOYD help lower costs, it's also an effective way to increase employee productivity!

These solutions are now available in packs. That's the idea behind "VDI-In-A-Box". Obviously, companies will have to handle security for these "application centers". The GCN article "Bring your smart phone to work; leave your data in Somalia" sheds some interesting light on this topic.

The only hitch with this kind of technology is that you need network access. But this isn't, or more accurately, will no longer soon be a problem. Indeed, 3G networks offer increasingly high performance, and with the arrival of LTE (or "4G"), coverage and speeds will only increase. You can read more about 4G's arrival in Europe here.

conclusion

The question is no longer "to BYOD or not to BYOD," but how and under **what security conditions**. Workplace virtualization solutions and applications joined with high-performance network access should help answer this question.

original article

http://oran.ge/ULp1tv

mobile security: wrapper or container?

by Philippe Macia

After our article on BYOD and security questions raised by personal tablets and mobile phones in the workplace, what changes are taking place concerning the **security of company applications** and communications on personal mobile phones?

More and more, companies are letting employees receive their work e-mails on personal tablets and smartphones. However, some are still wary about providing access to professional applications and documents from personal devices, especially because of security issues.

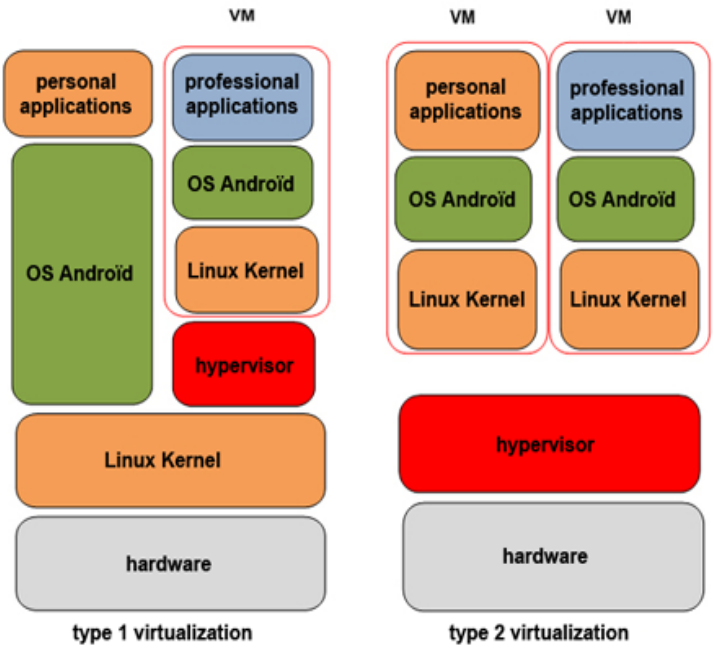
In this article, I'll talk about containers and wrappers, which are **two ways to separate personal and professional use** on a single device (smartphone or tablet). Both these methods are increasingly common on the market.

the container: its principles and derivatives

The idea behind containers is pretty simple: the point is to store professional applications and data in a zone that is completely separate from personal use. The advantage is that n**o data will exit the professional zone** and enter the personal zone.

But things start to get a bit tricky when you try to set up this solution.

There are **two different types**:
• type 1 virtualization: this installs a hypervisor to run a virtual machine complete with a kernel, an operating system (OS), and the professional applications located on top of the hardware layer and original kernel
• type 2 virtualization: this installs a hypervisor on top of the hardware layer to run two virtual machines, each containing a kernel, an OS and professional applications



advantages and disadvantages of containers

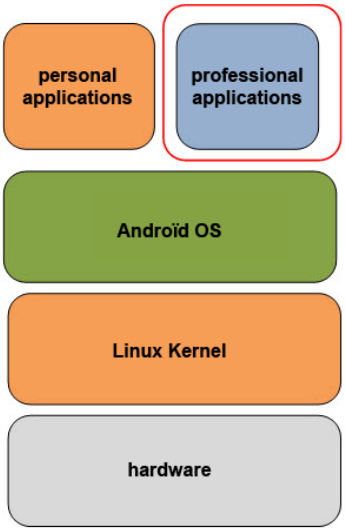
While the advantages are fairly obvious (high level of security, since data remains encrypted even if the device is lost or stolen), containers still present a few major disadvantages:

- **complex installation** (changes to be made on the phone and the terminal's ROM)
- currently only available on Android
- uses a lot of energy and processing power, thus reducing battery life and **significantly impacting the end user's experience**

good to know

These solutions have a significant impact on the end user's experience!

the wrapper, or sandbox



solution using a wrapper

The idea here is based on Java and its famous virtual machine, but we can also call this solution a sandbox or wrapper.

Basically it's **an application that controls the professional area in a secure bubble**. All applications running from the sandbox are secure because they are directly controlled by the sandbox. Similarly, documents are encrypted and can only be shared between applications within the sandbox. The system's security policy can be managed with an administration tool.

The secured application, or the wrapper, is then made available to the user through the company's private application store or through an MDM solution.

advantages and disadvantages of wrappers

The advantage of this model is that, in theory, you can **control applications running on any OS**. This includes applications developed using HTML 5, because special browsers are often developed for the professional zone to control access to mobile sites and/or websites, and thus limit the spread of malicious scripts.

The disadvantages of these types of solutions:
• while lighter than containers, wrappers still require **changes to be made on the device** through an application installation (but no need to modify the ROM)
• all applications secured by a wrapper must be recompiled, which can be time-consuming, even with tools supplied by editors
• the user experience must change because these tools differ from the originals (different e-mail and browser tools from the ones supplied by the manufacturer)

conclusion

The two approaches are interesting but **do not provide the same level of security**. Companies that need to give employees access to highly sensitive data should opt for container solutions, while applications secured by wrappers will still meet the security needs of most companies.

I also want to emphasize that these solutions have **a significant impact on smartphone performance**, so they should only be used with high-end devices that have fast processors and long battery life.

original article
http://oran.ge/VstiX0

about authors

Jean-François Audenard

Within Orange Business Services, I'm in charge of securing our cloud computing solutions and services. I'm the passionate kind and only look at things this way: no 50/50 for me, I'm an engaged and engaging blogger, I like to go off the beaten track. Sincerity is my tone and optimism and voluntarism my two engines

Philippe Macia

After previously working as a training manager, on-site IT officer, pre-sale technical officer, and customer service manager, I joined the Orange Business Services security team as a product manager.

I'm very committed to the user experience and easy administration of the solutions we create. My watchwords: knowledge sharing, logic, pragmatism and simplicity.

Vincent Maurin

I work for Orange Business Services as a security leader within Products and Services Development. My previous jobs as a technical “worker bee” lead me to pay specific attention to the difficulties of implementing companies’ security strategies and policies. Security, efficiency and pragmatism are my main pillars.

our blog:
http://blogs.orange-business.com/connecting-technology/

document available for download at:
http://knowledge-center.orange-business.com/

Edited by Orange Business Services
16.01.2013

France Télécom – 78, rue Olivier de Serres, 75015 Paris, France – SA au capital de 10 595 541 532 – 380 129 866 RCS Paris – Document non contractuel – juin 2012

Business Services

orange™