EDITOR: Rick Kuhn, NIST, kuhn@nist.gov

Securing BYOD

J. Morris Chang, *Iowa State University*
Pao-Chung Ho and Teng-Chang Chang, *Institute for Information Industry, Taiwan*

In the corporate world, Bring Your Own Device (BYOD) is becoming increasingly common, changing how we work. According to a 2012 Intel study of 3,000 IT managers and 1,300 users, productivity is viewed as the biggest benefit of BYOD.[1] An IBM Flexible Workplace Study reported increases in productivity of 20 percent or greater stemming from BYOD practices—the equivalent of an extra day of work per week.[2] BYOD lets employees use their personal device to work seamlessly across their personal user space and enterprise workspace instead of using multiple devices depending on business need, location, and circumstances.

Yet today's IT departments are concerned with the popularity of BYOD, because mixing personal and enterprise data presents security threats to corporate proprietary information. Enforcing the usage of two different mobile devices—one corporate and one personal—could mitigate this threat, but this strategy faces employee resistance because it's inconvenient. This creates a need for IT departments to develop company security policies that let employees access sensitive resources using personal devices.

The Challenges

In a survey of 2,100 individuals, conducted by Webroot, 41 percent said they use a personal smartphone or tablet for work purposes.[3] Furthermore, 70 percent of those smartphones and tables used for work had no additional security other than what was installed when the employee first purchased the device. According to another survey, 98 percent of employers claim to have a mobile security policy in place for accessing corporate data,[3] yet BYOD users tend to choose usability over security when it comes to selecting mobile applications. Device security, malware, and enforcement are major security concerns raised by BYOD.

Device Security

Security issues arise at all layers—including the network layer—but the main issues are at the device layer. Enterprise apps on a mobile device can leave company data on that device, presenting a major threat if the device is ever lost or stolen. Furthermore, if the user mixes personal and enterprise data, it could lead to data leakage if company information is accidentally sent to personal contacts.

Malware

Another concern is malware. The total number of known Android malware samples increased more than 10 times between July 2012 (about 45,000 samples) and January 2014 (about 650,000 samples).[4] These malwares tend to steal personal information, issue premium SMSs (which result in a fee for the sender) for financial gain, or engage in denial-of-service attacks. The malware might not specifically target enterprise data, but it creates concerns about backdoor data leakage for BYOD scenarios.

Enforcement

Personal devices used for work are part of the enterprise network, so it's essential to ensure that all mobile devices comply with enterprise security policies. However, it's difficult to enforce corporate policies on personal devices. The problem is exacerbated by the large variety of device hardware and fragmentation of the operating system. Moreover, security policies can change from time to time to cope with new security threats. Thus, effective security enforcement requires constant updating of both corporate and personal devices.

1520-9202/14/$31.00 © 2014 IEEE Published by the IEEE Computer Society

Secure Mobile Browsing

Although a virtual private network can be an effective way to maintain corporate security, administrators can also let employees access corporate intranet sites through the AirWatch Browser on employee-owned devices. A single sign-on and app tunneling lets users connect the AirWatch Browser to enterprise intranets and third-party Web filters.

Current Solutions

The following solutions and practices can help address BYOD security issues.

Security Policies

Typically, company BYOD policies include identifying which devices can be used in the company network, listing both allowed and banned apps, and describing classes of data that shouldn't be stored locally after being used by a mobile app. Companies also implement security policies (such as passwords or screen locks) for all devices and have strategies for lost or stolen devices and for when employees leave the company.[5] Furthermore, although a company might assume it owns the apps and data, the device owner might think differently.

The US White House published a BYOD policy on August 2012 that presents three high-level suggestions for implementing BYOD programs.[6] The first suggestion is to use *virtualization* to remotely access computing resources at a corporate facility, so corporate data isn't stored and corporate apps aren't processed on personal devices. The second suggestion is to implement a *walled garden*, so corporate data and apps are processed separately from personal data. The final suggestion is to apply *limited separation*, letting users mix corporate and personal data on a personal device while ensuring a minimal level of security controls.

Mobile Device Management

Mobile Device Management (MDM) tools are available commercially to manage mobile devices and enforce company security policies on such devices. Vendors such as VMware, MobileIron, and FiberLink provide MDM services specifically for BYOD.

Products, such as Maas360 by FiberLink, typically use a device enrollment process to register the personal device into the MDM program. This lets administrators manage the devices remotely. It might set customized authentication checkpoints on apps or data or restrict certain device features and settings. Some products (such as AirWatch by VMware) also provide Mobile Application Management (MAM) and Mobile Content Management (MCM) in addition to MDM. They can also wipe the device of enterprise content if necessary. Another technique—secure mobile browsing—is discussed in the related sidebar.

Separation Techniques

Techniques based on virtualization and on the operating system (OS) to separate enterprise space and personal space have shown potential.

In a BYOD scenario, private personal apps and data and important enterprise apps and data are contained and running on the same device. A BYOD design requires that the personal user space in no way compromise the security of the enterprise workspace. On the other hand, the enterprise workspace should in no way compromise the privacy of the personal user space. How to effectively separate the two spaces on the same mobile device becomes crucial for a successful BYOD design. Techniques, including virtualization, dual boot, and recently proposed virtual mobile platforms, can be used to achieve the separation goal. All of these techniques have their own advantages and drawbacks.

Vitualization. With hardware virtualization, hardware resources on a mobile device can be multiplexed to host multiple virtual machines. A type 1 (T1) hypervisor runs directly on the system hardware and provides a virtualized platform to host multiple guest OSs (here, the guest OSs would be the personal OS and the enterprise OS). This provides the best separation between the personal user space and enterprise workspace. However, this solution suffers from great performance degradation due to T1 overhead.

A type 2 (T2) hypervisor can also be used to provide system separation. In this case, the hypervisor runs on top of the original mobile device OS, while the enterprise workspace runs as a VM on the hypervisor. An example of this design is the VMWare Mobile Workspace (www.vmware.com/mobile-secure-desktop/overview). This solution provides more flexibility and is more user friendly, because the user can simply install the hypervisor as an app in the original OS. However, the enterprise workspace will be at risk if the original OS is compromised.

To enhance system performance, OS virtualization can be used to provide light-weight separation. In this case, kernel-level device namespaces are created to provide data isolation and hardware resource (device driver) multiplexing, allowing multiple virtual mobile devices to run on a single OS instance. An example of this design is Cells from Columbia University.[7] OS virtualization can improve the system

performance compared to hardware virtualization, but the adopter of this technique should keep in mind that both the personal user space and enterprise workspace can be compromised if an attacker targets the OS kernel.

Dual boot. This possible solution for device separation involves installing two OSs in different partitions on the same device. This process is just like performing traditional dual boots on desktops. Canonical provides a dual boot app[7] that modifies an Android device to let users switch between different OSs. OS dual boot provides a clean separation, but the long switching time degrades usability.

Virtual mobile platforms. The Remotium Virtual Mobile Platform provides another way to separate the personal user space from the enterprise workspace using the idea of remote control (www.remotium.com). This is similar to Microsoft Windows' remote desktop connection. In the Remotium solution, all enterprise data and apps run in secure virtual machines at Remotium's or the enterprise's datacenter. Employees can then set up remote connections to the virtual machines through a Remotium mobile client installed on each employee's mobile device. This is a simple and effective approach to improve enterprise data security, because no data is stored locally on the mobile device. Note, however, that this solution requires a constant Internet connection, and performance is determined by the Internet speed.

Including BYOD security in corporate IT management policies is inevitable, and companies must determine support capabilities, educational needs, and deployment phases. At the same time, they must separate personal and organization data and clearly define device requirements. Technologies that support BYOD must be evaluated based on performance, separation, and usability. Management policies for mobile devices and apps must be inclusive, enforceable, and updated constantly. BYOD might come with a high initial cost, but the payoff should be worth it in the long run. IT

To enhance system performance, OS virtualization can be used to provide light-weight separation.

References

1. "Insights on the Current State of BYOD," Intel, Oct. 2012; www.intel.com/content/www/us/en/mobile-computing/consumerization-enterprise-byod-peer-research-paper.html.
2. "Achieving Success with a Flexible Workplace: 2012 IBM Flexible Workplace Study," IBM Center for Applied Insights, May 2012; http://www.935.ibm.com/services/us/en/it-services/workplace-services/flexible-workplace.
3. "Fixing the Disconnect Between Employer and Employee for BYOD (Bring Your Own Device)," Webroot, July 2014; www.webroot.com/shared/pdf/WebrootBYODSecurityReport2014.pdf.
4. V. Svajcer, "Sophos Mobile Security Threat Report," SOPHOS, 2014; www.sophos.com/en-us/medialibrary/PDFs/other/sophos-mobile-security-threat-report.pdf.
5. J. Hassell, "7 Tips for Establishing a Successful BYOD Policy," *CIO*, 17 May 2012; www.cio.com/article/2395944/consumer-technology/7-tips-for-establishing-a-successful-byod-policy.html.
6. "Bring Your Own Device," The White House, 23 Aug. 2012; www.whitehouse.gov/digitalgov/bring-your-own-device.
7. C. Dall et al., "The Design, Implementation, and Evaluation of Cells: A Virtual Smartphone Architecture," *ACM Trans. Computer Systems*, vol. 30, no. 3, 2012, article; http://doi.acm.org/10.1145/2324876.2324877.
8. "Announcing Ubuntu and Android Dual Boot Developer Preview," Ubuntu, 23 Dec. 2013; http://developer.ubuntu.com/2013/12/announcing-ubuntu-and-android-dual-boot-developer-preview.

J. Morris Chang *is an associate professor at Iowa State University. His research interests include cyber security, wireless networks, and energy efficient computer systems. He is a senior member of IEEE. For further details, visit his webpage www.ece.iastate.edu/~morris or contact him at morris@iastate.edu*

Pao-Chung Ho *is the Executive Vice President of the Institute for Information Industry, Taiwan. His research interests include embedded systems, database systems, wireless communication networks, cybersecurity, and the Internet of Things. Contact him at pcho@iii.org.tw.*

Teng-Chang Chang *is a senior manager in the Smart Network and System Institute of the Institute for Information Industry, Taiwan. His research interests include next generation portable device, machine learning, and intelligent computer vision systems. Contact him at norman@iii.org.tw.*