A review on BYOD solutions and corporate security systems

P. de las Cuevas

Departamento de Arquitectura y Tecnologa de Computadores. Escuela Tcnica Superior de Ingenieras Informtica y de Telecomunicacin. CITIC. University of Granada, Spain

A. M. Mora

Departamento de Arquitectura y Tecnologa de Computadores. Escuela Tcnica Superior de Ingenieras Informtica y de Telecomunicacin. CITIC. University of Granada, Spain

1. Introduction

The rest of the paper is organized as follows. Next section presents some preliminary concepts and background of the work. Section defines the problem itself, describing the competition rules, along with the Infinite Mario Bros. platform, regarding the main features that the agent must consider and its constraints. Then, Section introduces the agents' approaches which will be analyzed in the paper, along with the set of experiments conducted to perform this analysis (Section jarl). Finally, Section describes the reached conclusions.

2. Preliminary concepts and background about mobile security

In computer security, each part of the system architecture and system software needs to be secured on its own. In client/server architecture it is necessary to distinguish between the following:

1. **Computer security.** Devices that are provided to the employee by the enterprise, are usually pre-configured and maintained by the IT department. These devices have installed antiviruses and other software that normally blocks malware. Those owned by the employees, but allowed by the enterprise (BYOD circumstances), should satisfy a number of prerequisites imposed by the company.
2. **Network security.** Taking into account the security inside the enterprise network, before accessing the internet, the model that is more often used could be like the one presented in Figure 1.1. The secured access

Email addresses: paloma@geneura..ugr.es (P. de las Cuevas), amorag@geneura.ugr.es (A. M. Mora)

network is generally divided into untrusted and trusted zones. As it can be seen in figure 1.1., there are border routers, firewalls, network address translation (NAT), intrusion detection system (IDS), intrusion prevention system (IPS), antivirus, and proxies between the trusted and untrusted zones within a network. Regarding firewalls, they are typically installed between the untrusted public Internet and the private LANs so that only desired traffic is allowed between these two networks. The zone with an intermediate trust level, situated between the Internet and a trusted internal network, is often referred to as a perimeter network or demilitarized zone (DMZ).

3. **Security programming.** This type of programming has been defined as the combination of secured programming and safe programming. This is, the application needs to secure or assure the operations, and so should not damage the system (it is safe).
4. **Database security.** Regarding to the database, it can be secured by taking care of the user identification and authentication, controlling the access to some objects, auditing the activities that are happening with the objects, and solve security issues such as the management of data system integrity, reliability or availability.

2.1. Enterprise managed solution

Here we explain the security architecture model of an enterprise with an intranet WiFi network.

2.2. Outsourced solution

In this subsection we explain the security architecture model of an enterprise in which some of the mobile services have been outsourced to an external operator.

3. Tools for corporate mobile security

Now that BYOD philosophy is a trend, a number of tools have been designed specifically for CSOs and Chief Information Security Officers (CISOs) to secure, monitor, and control spartphones and other personal mobile or portable devices. Some of these tools have influenced the development of the MUSES project itself. This section presents the products that can be considered related to MUSES objectives.

3.1. IBM Hosted Mobile Device Security Management

One of the first companies who supported the BYOD model was IBM in 2011, as they recognized the increase of employees who brang their personal smartphones or tablets into the workplace. To help organizations embrace both company and employee owned mobile devices (this practise is part of the bring-your-own-device model) in a security-rich environment, IBM developed a mobile device security management solution. For IBM, a mobile security strategy should focus on several key areas:

1. Data and resources accessible from mobile devices the organization should identify which business data it will allow to be stored and processed on which mobile devices. This helps determine what needs to be protected and to what degree.
2. Platform support because different mobile platforms have different native security mechanisms, the organization needs to determine which mobile device platforms will be allowed in the business environment and, thus, need to be supported in the mobile security strategy and plan.
3. Management methodology there is need to decide the responsibility for mobile security management work, whether using the current IT security team to handle mobile devices, or outsourcing to a managed security service provider.
4. Best practices - no matter what the mobile environment, a number of mobile security policies and best-practice procedures need to be put in place and should also be identified in the companys mobile security strategic plan.

Taking into account these considerations, IBM has developed a framework that specifies security domains and levels for applying various security technologies. When applied to mobile devices, the framework suggests the following security controls, with actual requirements varying by deployment:

1. Identity and access:
   (a) Enforce strong passwords to access the device.
   (b) Use site authentication or two-factor user authentication to help increase the trustworthiness between a user and a website.
   (c) If VPN access to corporate intranet is allowed, include capability to control what IP addresses can be accessed and when re-authentication is required for accessing critical resources.
2. Data protection:
   (a) Encrypt business data stored on the device and during transmission.
   (b) Include capability to wipe data locally and remotely.
   (c) Set timeout to lock the device when it is not used.
   (d) Periodically back up data on the device so data restore is possible after the lost device has been recovered.
   (e) Include capability to locate or lockout the device remotely.
3. Application security:
   (a) Download business applications from controlled locations.
   (b) Run certified business applications only.
   (c) Monitor installed applications and remove those identified to be untrustworthy or malicious.
4. Fundamental integrity control:
   (a) Run antimalware software to detect malware on storage and in memory.
   (b) Run a personal firewall to filter inbound and outbound traffic.

(c) Integrate with the companys VPN gateway so a devices security posture becomes a dependency for intranet access.

5. Governance and compliance:
   (a) Incorporate mobile security into the companys overall risk management program.
   (b) Maintain logs of interactions between mobile devices and the companys VPN gateway and data transmission to and from servers within the intranet.
   (c) Include mobile devices in the companys periodic security audit.

Regarding IBM hosted mobile device security solutions architecture, the solution is built on a sound client-server architecture in which the server centrally controls and manages security policies and settings for various security features. The client would be installed on the mobile device and regularly communicate with the server to enforce policies, execute commands and report status. Also, IBMs solution contains reporting and analysis capabilities, with information that helps the company to support policy and regulation compliance, recognize the mobile threat landscape and evaluate the solutions effectiveness in countering threats.

3.2. Sophos Mobile Control

Sophos is a company founded in 1985 focused on IT security and data protection for businesses. Their Mobile Device Management main product is Sophos Mobile Control. Sophos Mobile Control is oriented to IT administration for mobile devices. Sophos offers to the users the possibility of choosing the delivery model to suit their needs, i.e., between on-premise and Software as a Service (SaaS). The features of this tool are the following:

1. Mobile Device Management The tool offers the possibility of managing all workers and co-workers smartphones and tablets from a single-based console. The console monitors the devices throughout their full lifecycle: from the initial set up and enrolment, right through to decommissioning. Other features are:
   (a) It is possible also to connect to an existing user directory using Lightweight Directory Access Control (LDAP). LDAP is an application protocol for accessing and maintaining distributed directory information services over an Internet Protocol (IP) network.
   (b) Configure policies for the devices and deploy them over the air.
   (c) Turn on the built-in security features for iOS, Android, Windows and BlackBerry devices, including password protection and encryption.
   (d) Drill down to the individual settings for all registered devices for configuration, serial numbers, model and hardware details, installed applications and much more.
   (e) Manage your apps with an included Enterprise App Store.
   (f) Use a dashboard to get the status of the devices at-a-glance.

(g) Define which features are available to the workers using a self-service portal.
(h) Initiate mitigation actions in case of loss or theft, such as lock, wipe, remote alarm and SIM change notification.
(i) Locate Android and iOS devices.

2. Mobile Security Additional security is provided by the incorporation of Malware and Web protection. Although, this feature is optional.
3. Compliance Enforcement The main goal is not to sacrifice companys security in favour of flexibility for the users. Companys BYOD initiative should include an Acceptable Use Policy to ensure the users are aware of any measures the company may take if a device breaches the security policies. This is reachable by doing three main tasks:
   (a) Enforce Security Policies: Sophos Mobile Control allows setting up user and group-based security policies. The security settings can also vary from one platform to another. Set task bundles and individual actions for many different violations.
   (b) Risk mitigation: these actions can be set according to the severity of a breach. For minor cases, the company may want to simply inform the user. If sensitive data is at risk, a remote wipe may be the only viable option. The actions vary for each platform, but the most common platforms such as Android and iOS allow blocking email access, notifying the admin, performing a remote lock or wiping, locating a device using 3D maps, triggering a remote alarm, transferring a task bundle combining a number of actions, and Sophos Mobile Security adds the possibility of trigger a scan.
   (c) Compliance check: the settings available in the compliance check vary for each platform. Some of the most widely used features include allow or disallow root rights or jailbreaking, allow/disallow app downloads from non-market app stores, require encryption, and whitelist or blacklist apps. Additionally, Sophos Mobile Security allows disallowing malware apps, set maximum intervals since last Mobile Security scan, and allow or disallow suspicious apps and potentially unwanted apps (named PUAs).
4. Mobile Application Management The Enterprise App Store in Sophos Mobile Control allows the company to supply the users with recommended and required apps directly on their device. Both companys in-house and app store apps are shown on the users mobile device, where they can click to trigger the installation.
5. User Self-Service One of companys goals is to keep the employees working without increasing the burden for the IT department. The self-service portal built-in included in Sophos Mobile Control has the following features:
   (a) Allow users to register their own devices and agree to an acceptable use policy that the company has defined.

(b) Let them use their personal device as part of the BYOD program, and the company can make sure it is secured.
(c) The users can choose to remotely locate, lock or wipe their devices and reset their passcode without having to contact the company help desk.
(d) Provide a simple step-by-step process when they register a device. All profiles, including email access, are available immediately after registration.
(e) The company define which features are available in its self-service portal from the administrator console.
(f) The users can access the portal from their mobile device or from any PC with Internet access.

6. Easy configuration and maintenance Sophos provides an easily install and maintain control with over-the-air setup and configuration from a web console.

3.3. Good's Bring Your Own Device solution

Good Technology is a company that was founded in 1996 in California. They provide Push e-mail (for further explanation, see Chapter 8: Glossary), see and mobile device management and security products for mobile phones. The philosophy followed by Good is similar to Samsungs Knox one: to create a secure container that places an unreachable partition between personal and business data to protect email and other programs. The solutions that they offer are:

1. Let the employees choose the smartphone, tablet, or other mobile device they want to use.
2. Protect user privacy and critical information by using a secure container to separate personal and company data.
3. Cut device and carrier costs by running a BYOD program that reduces the need for company-owned devices.
4. Block unauthorized devices from the companys network by leveraging Goods secure Network Operations Center (NOC).
5. Provide access to secure collaboration solutions (email, PIM, calendar), intranet, and in-house or third-party mobile applications.
6. Offer best practice recommendations to help the company's bring-your-own-device policies such as reimbursements and stipends. There is a document available at Goods webpage (at `http://www1.good.com/mobility-management-solutions/bring-your-own-device`) which contains a number of questions about security policies and how to cope them all.

3.4. Samsung's Knox Mobile Security Suite

As part of its SAFE (Samsung for enterprise) brand, Samsung revealed at the Barcelona Mobile World Congress 2013 the Knox application, which will be available on his next Galaxy smartphone generation. The main feature of

this security package is the use of different containers for the business and the personal side. Each one even has its own set of wallpapers, in order to be more evident for the user. Figure 1 shows the architecture followed by the application. To enter the business side, it will be necessary to introduce a password. Nevertheless, no passwords will be required for the business applications anymore. The applications approved by the company IT department must meet Samsungs security standards and allow single sign-on. There will be over 338 IT policies that can be access via the Knox API. Also, Knox allows different VPNs for individual apps. Regarding the information protection methods, data files saved by applications of each environment are encrypted with AES 256-bit algorithm, in such manner the container and only the container can access these files. In the same way, the user wont be able to share data between the two environments:

1. There will be separate contact lists and the user cannot send a contact from one side to the other.
2. If the user copies data to the clipboard in the Knox container, it wont be there in the personal container.

Other features of this tool are the following:

1. Customizable Secure Boot This ensures that only verified and authorized software can run on the device. It is a primary component that forms the first line of defence against malicious attacks on devices with Samsung KNOX. In addition, Samsung Knox's Secure Boot technology allows the switch of the secure boot root certificate in a secure manner after the devices are shipped.
2. TrustZone-based Integrity Measurement Architecture (TIMA) This runs in the secure-world and provides continuous integrity monitoring of the Linux kernel. When TIMA detects that the integrity of the kernel or the boot loader is violated, it takes a policy-driven action in response. One of these policy actions disables the kernel and powers down the device.
3. Security Enhancements for Android This feature provides an enhanced mechanism to enforce the separation of information based on confidentiality and integrity requirements. It isolates applications and data into different domains so that threats of tampering and bypassing of application security mechanisms are reduced while the amount of damage that can be caused by malicious or flawed applications is minimized.

3.5. BlackBerry Balance

This security package was announced as a feature of BlackBerry 10. Nevertheless, it is available with BlackBerry Enterprise Service 10, which is a device management, security and app management for BlackBerry, iOS and Android devices. When BlackBerry Balance it is activated, these characteristics are available:

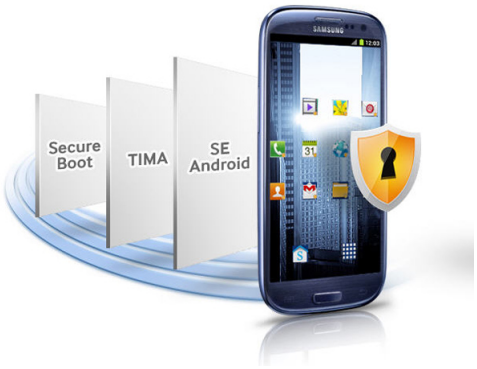

Figure 1: Samsungs Knox utility architecture. Source: `http://www.samsung.com/global/business/mobile/solution/security/samsung-knox`.

1. Work data cannot be copied and pasted into personal apps. The device will display messages like the shown in Figure 2.
2. If a user attempts an action that is not permitted by IT policy or that may cause secure work information to come into contact with personal applications, the action wont be permitted.
3. Employees can access the personal information and apps that keep them in touch with the people and things they care about, while staying connected to important work information when they need to perform.
4. If the device gets lost or stolen, or if the employee leaves the organization, there will be an option to wipe just work information and it can be done remotely.

3.6. Multiplatform Usable Endpoint Security

MUSES will provide a device independent, user-centric and self-adaptive corporate security system, able to cope with the concept of seamless working experience on different devices, in which a user may start a session on a device and location and follow up the process on different devices and locations, without corporate digital asset loss. The final product of MUSES for companies will be a system which will be installed in workers and co-workers devices, and also on enterprise servers, following the classical client-server system architecture. This means that there are going to be several types of MUSES inside the final product:

1. Desktop devices, these are computers and laptops that the employees have in their offices.
2. Mobile devices, including smartphones and tablets owned by the employees of the enterprise and also by the co-workers. The co-workers are indirect employees of the company, i.e. workers of an external company that are

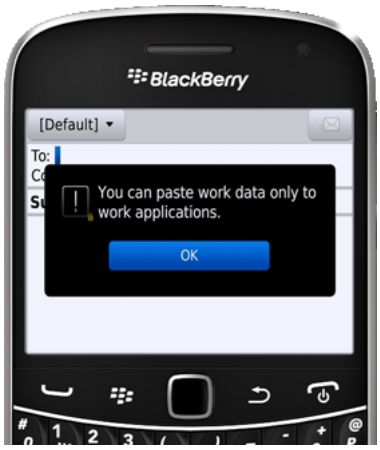

Figure 2: Displayed message in new Blackberry 10 when attepmting to copy sensitive company data. Source: `http://uk.blackberry.com/business/software/blackberry-balance.html`.

hired occasionally by the first one, or have to perform some activities inside the company, e.g. maintenance activities.

3. Enterprise side services and applications - inside the company server, a MUSES manager will be implemented to control the MUSES workflow with the mobile devices. Security policies would go on this side.

Thus the system will be implemented at two high levels: client and server. Client or device side is related to the end user, normally, an employee who uses a portable and mainly personal device to access enterprise resources. The system should prevent her from using the device incorrectly from the enterprise security (respecting its security policies) point of view. Thus MUSES will monitor her context and behaviour, and control her actions, letting or forbidding them depending on those policies. Server side is controlled by an enterprise security manager, the Chief Security Officer (CSO), who defines the security rules to consider in the system according to the company security policies. In addition, this server will receive, store and process all the gathered information from the users devices. The process will analyse the data, performing a real-time risk and trust analysis and also (adapted) event-correlation tasks, trying to predict users malicious or non-secure behaviours.

One goal of the project is to be a multi-platform approach; that is, MUSES solution should be deployable and run on different platforms. Being multi-platform is an important requirement for adaptation of MUSES in a wide range of corporate security strategies.

4. Conclusions

In this work, Bla, bla, bla

Acknowledgements

This work has been supported by MUSES FP7 project, and in part by the P08-TIC-03903 project awarded by the Andalusian Regional Government, the FPU Grant 2009-2942 and the TIN2011-28627-C04-02 project, awarded by the Spanish Ministry of Science and Innovation.

References

[1] Bäck, T., *Evolutionary algorithms in theory and practice*, Oxford University Press, 1996.

[2] R. Baumgarten, *Mario AI A* agent*, http://www.doc.ic.ac.uk/ rb1006/projects:marioai.

[3] Bojarski, S., Bates-Congdon, C., *REALM: A Rule-Based Evolutionary Computation Agent that Learns to Play Mario*. In: Proceedings of the 2011 IEEE Symposium on Computational Intelligence and Games (CIG 2011), IEEE Press, pp. 83–90, 2011.

[4] Booth, T.L., *Sequential Machines and Automata Theory*, John Wiley and Sons, Inc., New York, 1st edition, 1967.

[5] Goldberg D.E., Korb B., Deb K., *Messy genetic algorithms: motivation, analysis, and first results*, Complex Systems, 3(5), pp. 493–530, 1989.

[6] Hagelbäck, J., *Potential-Field Based navigation in StarCraft*. In: Proceedings of the 2012 IEEE Symposium on Computational Intelligence and Games (CIG 2012), IEEE Press, pp. 388–393, 2012.

[7] Jang, S.H., Yoon, J.W., Cho, S.B., *Optimal strategy selection of non-player character on real time strategy game using a speciated evolutionary algorithm*. In: Proceedings of the 5th IEEE Symposium on Computational Intelligence and Games (CIG'09), IEEE Press, pp. 75–79, 2009.

[8] Laird, J.E, *Using a computer game to develop advanced AI*. Computer, 34(7), pp. 70–75, 2001.

[9] Martn, E., Martnez, M., Recio, G., Saez, Y., *Pac-mAnt: Optimization based on ant colonies applied to developing an agent for Ms. Pac-Man*. In Proc. 2010 IEEE Conference on Computational Intelligence and Games (CIG 2010), IEEE Press, pp. 458–464, 2010.

[10] Mora, A.M., Moreno, M.A., Merelo, J.J., Castillo, P.A., Garca-Arenas, M.I., Laredo, J.L.J., *Evolving the cooperative behaviour in Unreal^{TM} bots*. In Proc. 2010 IEEE Conference on Computational Intelligence and Games (CIG 2010), IEEE Press, pp. 241–248, 2010.

[11] Mora, A.M., Fernndez-Ares, A., Merelo, J.J., Garca-Snchez, P., *Dealing with noisy fitness in the design of a RTS game bot.* In Proc. Applications of Evolutionary Computing: EvoApplications 2012, LNCS, vol. 7248, Springer, pp. 234–244, 2012.

[12] Pedersen, C., Togelius, J., Yannakakis, G., *Modeling Player Experience in Super Mario Bros.* In Proc. 2009 IEEE Symposium on Computational Intelligence and Games (CIG'09), IEEE Press, pp 132–139, 2009.

[13] Pepels, T., Windans, H.M., *Enhancements for Monte-Carlo Tree Search in Ms Pac-Man.* In Proc. 2012 IEEE Conference on Computational Intelligence and Games (CIG 2012), IEEE Press, pp. 265–272, 2012.

[14] Ponsen, M., Munoz-Avila, H., Spronck, P., Aha, D.W., *Automatically generating game tactics through evolutionary learning.* AI Magazine, 27(3), pp. 75–84, 2006.

[15] Shaker, N., Nicolau M., Yannakakis, G.N., Togelius, J., O'neill, M., *Evolving Levels for Super Mario Bros Using Grammatical Evolution.* In Proc. 2012 IEEE Symposium on Computational Intelligence and Games (CIG 2012), IEEE Press, pp 304–311, 2012.

[16] Small, R., Bates-Congdon, C. *Agent Smith: Towards an evolutionary rule-based agent for interactive dynamic games.* In Proc. 2009 IEEE Congress on Evolutionary Computation (CEC'09), pp. 660–666, 2009.

[17] Spronck, P., Sprinkhuizen-Kuyper, I., Postma, E., *Improving opponent intelligence through offline evolutionary learning.* International Journal of Intelligent Games and Simulation, 2(1), pp. 20–27, 2003.

[18] Synnaeve, G., Bessire, P., *A Bayesian Model for RTS Units Control applied to StarCraft.* In Proc. 2011 IEEE Symposium on Computational Intelligence and Games (CIG 2011), IEEE Press, pp 190–196, 2011.

[19] Togelius, J., Karakovskiy, S., Koutnik, J., Schmidhuber, J., *Super Mario evolution.* In Proc. 2009 IEEE Symposium on Computational Intelligence and Games (CIG'09), IEEE Press, pp 156–161, 2009.