POSTER: Preserving Privacy and Accountability for Personal Devices

Gabriela Gheorghe*
Indisciplinary Centre for Security, Reliability and Trust, University of Luxembourg
4 Rue Alphonse Weicker, L-2721 Luxembourg
gabriela.gheorghe@uni.lu

Stephan Neuhaus
Communication Systems Group
Eidgenössische Technische Hochschule Zürich
Gloriastrasse 35, 8095 Zürich, Switzerland
neuhaust@tik.ee.ethz.ch

ABSTRACT

Using personal mobile devices for work gave rise to a trend called "bring your own device", or BYOD. BYOD brings a productivity boost for employees, but also headaches for employers: on the one hand, the business has a legitimate interest in monitoring the device, in order to prevent security breaches by employees; but on the other hand, employees have a reasonable expectation of privacy when they use their devices for private functions. This poster presents our project called Privacy-Preserving Accountability for peRsonal Devices (PriPARD, pronounced "prepared"). PriPARD addresses the tension described above by designing and evaluating concrete privacy mechanisms for mobile devices used in a corporate environment. Instead of imposing a "privacy firewall" between users and the Internet, in PriPARD the aim is protecting user privacy within the corporate network and non-disclosure outside this network. PriPARD's vision is to gather practical experience with the tradeoffs between monitoring and privacy needs, to help both mobile device users and managers of corporate networks.

Categories and Subject Descriptors

C.2.0 [**Computer Communication Networks**]: General—*Security and Protection*; C.2.3 [**Computer Communication Networks**]: Network Operations—*network monitoring, network management*; D.4.6 [**Operating Systems**]: Security and Protection—*Access Controls*

Keywords

Privacy; Mobile Devices; Accountability; Policies; Bring your own device

1. MOTIVATION

BYOD means Bring Your Own Device in the company network (and work on it). Coupled with the tendency to "work from any location", this trend to "work from any of your devices" affects the way that IT infrastructures are designed and how their security properties should be managed. The SANS institute shows that employees prefer to use confortable devices instead of their company's devices, or even using work devices for private use - both approaches forbidden by the IT policy [10]. MobileIron acknowledges that device homogeneity in the enterprise is impossible and that current mechanisms to collectively secure such devices are either ineffective or privacy-unaware [8, 9]. Other mobile security surveys such as [14, 11] have shown that there are many organisations to create mobile applications for their customers, that they are already allowing employees to use their personal devices at work.

Organisations have most of their intellectual property and sensitive data in the datacentre and network where personal devices can reach [14]. In the face of so many new personal devices, the need for enterprise accountability is dire. Reports such as Ernst and Young's [5] admit that better accountability means more monitoring of personally identifiable information. For example, suspicious device behaviour can imply that the corporate data on a personal smartphone is at risk. But while monitoring device activity to rule out suspicious behaviour (e.g., sudden location change from one continent to another), the software polls periodically for device parameters that are not strictly needed (e.g., location in town); hence a privacy breach occurs if these parameters are stored in the network.

On a broader scale, data privacy is mentioned in the recent EU Data Protection Regulation (January 2012) mainly from the point of view of instating "appropriate measures" to protect private data leakage [9]. As usual with legal texts, laws refrain from defining what are "appropriate measures", "useful precautions of the data controller", "reasonable precautions to protect data accessed on personally owned devices", or "adequate protection". To put regulations into practice, cloud service providers push the responsibility to implement privacy and security measures to clients. In the meantime, massive government surveillance operations revealed to be taking place in the US [7] and UK [2] are pointing at the dire lack of privacy-enhancing technologies for users in their day-to-day life.

In terms of privacy tools for users, with PriPARD we want to start (relatively) small and focus on corporate networks and mobile devices. In practice, there are no procedures nor tools to protect privacy in a corporate network. Users cannot consent to data gathering because they are not even aware of the traces they leave online or in a corporate net-

*corresponding author

CCS'13, November 4–8, 2013, Berlin, Germany.

http://dx.doi.org/10.1145/2508859.2512500.

work. They do not know what applications produce and consume their private data locally, and where their data goes when sent away from their devices. As an ongoing project, PriPARD is the first to address and, where possible, solve the tension between the owner's privacy and an organisation's need to monitor. Its purpose is twofold: first, to examine how much private data is still gatherable when existing privacy controls (business containers, process sandboxing, etc.) are used on a mobile device. Second, assuming that mobile devices cannot be fully stopped from emitting some private data, PriPARD wants to build privacy into the system, in such a way that users can tune some of the private data emitted by their devices, and how that data is handled in the network.

2. STATE OF THE ART

In privacy management for mobile devices, most of the research efforts investigate single device mechanisms. The best known mechanism that tracks how sensitive information flows into the system is TaintDroid [4], built for the Android platform. TaintDroid aims to give visibility to device users over how their sensitive data is handled by smartphone applications at runtime at the level of variables, methods, file operations and messages among applications. Other than work building up on TaintDroid [1, 13, 6], very few papers on privacy mechanisms consider the "private data over the untrusted network" aspect: Smokescreen[3] is a privacy management system that uses different broadcast signals to allow users to control how they share their location with social contacts differently than with strangers. Mobishare [15] protects privacy in mobile online social networks, whereby the user location is anonymised and obscured when using untrusted location servers.

An interesting approach is taked by the European project PRISM[12]. PRISM aims to embed privacy preserving mechanisms into traffic monitoring technologies, especially those that perform anomaly detection in a network. The project makes the observation that it is hard to implement gathering personal data so that not too much private data is stored. Instead of doing first data gathering for anomaly detection and then anonymisation, PRISM's approach is to join the two together: a front-end performs fast analysis of raw data, and if needed it encrypts this data in a way that protects its privacy and yet that is reversible so that a back-end can de-anonymize and further analyse this data. Access control management for such data is based on semantic models comprising notions such as: purpose of requested data usage, types and identification of the requesting entity, intended processing, and applicable regulatory provisions. When deployed in the data controller domain, PRISM can capture and inspect all packet flows on the network link.

In terms of technologies on the market, Blackberry Balance[1] is a technology that manages work and home user profiles on BlackBerry devices. Using two separate encrypted file systems with a unified view of data, private applications cannot access corporate data, and vice versa. Email, calendar, contacts, organizer data, applications and files that are pushed on the device via a corporate channel are by default tagged as 'work'; users cannot reclassify work data as private data, but personal data can be reclassified as work data. The technology also allows for remote device wiping for the corporate profile, disallowing backups of work data (to prevent the reclassification of backed-up corporate data as private data), as well as disallowing browser traffic, depending on the Internet connection type. Unfortunately, BlackBerry Balance is a proprietary technology tighly linked with BlackBerry 10 OS and the BlackBerry Enterprise Server, and does not lend itself to privacy enhancements on the user side.

None of the works we have seen examine how to handle the private data of the user (i.e. device usage habits, applications and sensor data) once it is emitted by certain applications and out of the device into the network. This is an important aspect, especially as we know that personally identifiable information is being gathered without user consent because of the organisation's need to monitor the user. It is not clear from the state of the art what are the available defenses that users can install on their devices, and how well such defenses work to protect user privacy.

3. CONTRIBUTIONS

On the one hand, PriPARD will examine how much private data can still be gathered when existing privacy controls (TaintDroid and related solutions, business containers, process sandboxing, etc.) are used on a mobile device. We believe that personal data emitted by user devices should be scrubbed off as much as possible before this data reaches the network, and PriPARD will examine if that is fully possible on modern mobile platforms. As current research does not examine the overall privacy of existing approaches as perceived by the user of the device, PriPARD will look for ways to allow employees to check what private information is emitted and gathered when they work. Hence PriPARD's first contribution to knowledge development is to raise device owner awareness about existing privacy-enabling tools to use on the devices on which they also work, as well as how these tools perform. Also, it is interesting to study what kind of device monitoring is still performed/needed when the device switches to a personal profile, and how sensor data is treated: can sensor data produced by an application running in work mode, be separated from data from the same sensor from a different application running in personal mode?

On the other hand, it is a given that a certain amount of control (or monitoring) should be exercised in the corporate network when the employee is working. Assuming that mobile devices cannot be fully stopped from emitting some private data (be it explicitly private or data that can be corroborated to infer private data), PriPARD wants to build privacy into the system, in such a way that users know of the private data emitted by their devices, as well as how that data is handled in the network. This approach will help find out if companies can give proofs to mobile device users of the network's compliance with user privacy preferences set up on their devices, but concerning the corporate network. Our vision is that whatever private data cannot be scrubbed off before reaching the corporate network, should be confined within the network and not sent to the Internet.

PriPARD's main objective is to build a management layer enforcing that employee private data does not leak outside the enterprise network. Such management tools should be partially controllable from the user devices when it comes to their private data. By linking mobile device mechanisms with network-level monitoring, PriPARD will make a novel contribution to the advancement of privacy mechanisms in

[1] `http://us.blackberry.com/business/software/blackberry-balance.html`

general. The point with privacy-conscious network monitoring, however, is not to have a centralised sink for this employee private data, but to have a distributed set of controls woven into the network fabric. In this way, it is more feasible to protect employee privacy, since it would be comparatively harder for a malicious employee to gain data about another employee. With its tools, PriPARD will contribute to knowledge development with practical experience with the trade-offs between security needs and privacy protection, for the corporate network managers.

4. IMPACT OF PROJECT AND POSTER

In all, PriPARD will investigate to what extent it is possible to design and build an open framework for managing personal mobile devices in a corporate network, with privacy mechanisms that the employees can use on their personal devices. We deem it is time to investigate what guarantees of enforcing privacy are essential to make users sure that the privacy settings on their devices will not be discarded at the level of the network. For example, a possible such tool is an application installable on mobile devices, that would show where the user's personal data is processed across the corporate network. We foresee that such mechanisms will span both Android middleware on devices - with minimal operating system changes needed since these devices are, after all, personal - but also endpoints of the corporate network.

On the long run, PriPARD wants to show that it is possible to give control to the mobile device users over the data they are generating about themselves, and also that it is possible for a company to manage potentially sensitive mobile user data (of its employees and customers). With proofs of concept on these topics, PriPARD can lead the way to a whole range of technologies for network policy-management that are privacy-aware and that allow, to a certain extent, mobile user tuning.

With this poster, we want to start a discussion with both researchers and companies on how to build configurable privacy-enhancing technologies for mobile devices in the BYOD setting. Our aim in this discussion is to find collaborations aimed at enhancing user awareness but also at helping companies improve their network management from the point of view of privacy protection.

5. REFERENCES

[1] M. Conti, V. T. N. Nguyen, and B. Crispo. Crepe: context-related policy enforcement for android. In *Proc. 13th intl. conf. on Information Security*, ISC'10, 2011.

[2] G. Corera. GCHQ data-tapping claims nightmarish, says German justice minister. `http://www.bbc.co.uk/news/uk-23017108`, 2013.

[3] L. P. Cox, A. Dalton, and V. Marupadi. Smokescreen: flexible privacy controls for presence-sharing. In *Proc. intl. conf. on Mobile systems, applications and services*, MobiSys '07, 2007.

[4] W. Enck, P. Gilbert, B.-G. Chun, L. P. Cox, J. Jung, P. McDaniel, and A. N. Sheth. Taintdroid: an information-flow tracking system for realtime privacy monitoring on smartphones. In *Proc. 9th USENIX conf. on Operating systems design and implementation*, OSDI'10, 2010.

[5] Ernst and Young. Privacy trends 2012 - The case for growing accountability. `http://www.ey.com/Publication/vwLUAssets/Privacy_trends_2012/\$FILE/Privacy-trends-2012_AU1064.pdf`, 2012.

[6] D. Feth and A. Pretschner. Flexible data-driven security for android. In *Proc. 2012 IEEE Sixth Intl. Conf. on Software Security and Reliability*, SERE '12, 2012.

[7] G. Greenwald. NSA collecting phone records of millions of Verizon customers daily. `http://www.guardian.co.uk/world/2013/jun/06/nsa-phone-records-verizon-court-order`, 2013.

[8] M. Iron. BYOD Strategies - Chapter 2. `http://www.webtorials.com/main/resource/papers/mobileiron/paper1/byod_part_2.pdf`, 2011.

[9] M. Iron. International Data Privacy Legislation Review: A Guide for BYOD Policies. `http://www.webtorials.com/main/resource/papers/mobileiron/paper5/Guide_for_BYOD_Policies.pdf`, 2012.

[10] K. Johnson. SANS Mobility / BYOD Security Survey. `http://www.sans.org/reading_room/analysts_program/mobility-sec-survey.pdf`, 2012.

[11] T. Kemp. As Mobile Device Management (MDM) Becomes Commoditized, What's Next for MDM? `http://www.forbes.com/sites/tomkemp/2013/02/19/as-mobile-device-management-becomes-commoditized-whats-next-for-mdm/`, 2013.

[12] PRISM project Consortium. PRIvacy-aware Secure Monitoring. `http://www.fp7-prism.eu/`.

[13] G. Russello, M. Conti, B. Crispo, E. Fernandes, and Y. Zhauniarovich. Demonstrating the effectiveness of moses for separation of execution modes. In *Proc. 2012 ACM conf. on Computer and communications security*, CCS '12, 2012.

[14] H. Schultze. BYOD and Mobile Security Survey Results. `http://www.slideshare.net/informationsecurity/byod-and-mobile-security-report-2013-19033467`, 2013.

[15] W. Wei, F. Xu, and Q. Li. Mobishare: Flexible privacy-preserving location sharing in mobile online social networks. In *INFOCOM*. IEEE, 2012.