

Comments of BlackBerry Limited

Mobile Security Project, Project No. P145408

BlackBerry Limited (“BlackBerry”) appreciates the opportunity to comment on the topics discussed previously by Adrian Stone, former Director of BlackBerry Security Response and Threat Analysis, during his participation in the FTC’s mobile security forum last year. Please find our comments below addressing questions from the (I) Secure Platform Design, (II) Secure Distribution Channels and (III) Secure Development Practices sections.

I. Secure Platform Design

- *How can platforms create robust development environments while limiting the potential for abuse by privacy-infringing or malicious third-party applications? Commenters may interpret the term “application” broadly to include any mobile software (e.g., native, web-based, etc.) that has access, via a platform, to consumers’ personal information or device resources.*

BlackBerry uses a multi-layered approach in order to provide a strong level of protection for our customers, including implementing practices and technologies for identifying malicious software and potential privacy impacts of applications being submitted for distribution on BlackBerry World. This approach includes an anti-malware strategy built on five core pillars including:

1) **BlackBerry’s built-in platform protections**

- a. Fundamentally, the effectiveness of a platform’s privacy controls relies on maintaining the integrity and security of the mobile operating system. A secure mobile operating system helps protect against malicious applications or attacks that leverage device software vulnerabilities to circumvent designed security and privacy controls for the purpose of exfiltrating sensitive information (data, personally identifiable information, location information, etc.). BlackBerry helps protect the BlackBerry operating system through the following approaches which include, but are not limited to:
 - i. **Hardware root of trust design principles and code verification techniques** that help protect the integrity of the operating system and installed applications each time it is loaded and also while running. These approaches increase platform security by mating software controls to hardware design, making it more difficult for attackers to compromise the security of the device.

- ii. **Secure Microkernel Architecture** - BlackBerry leverages its QNX secure microkernel, designed for resiliency, integrity and security, to help make the BlackBerry platform more resistant to attacks. Through careful, centralized design and control, this microkernel architecture also helps limit what damage malicious applications can do, if they were somehow to be installed.
 - i. **Secure Code Development Processes** – BlackBerry implements practices and technologies for secure code development and related testing activities that help limit vulnerabilities from reaching the production code environment.
 - b. BlackBerry devices are designed to provide customers visibility into an application’s behavior as well as provide users with notifications about what on-device resources an application accesses. This capability provides customers additional permission controls for all native apps downloaded on a BlackBerry device.
 - i. Application permissions that readily empower consumers to make better informed decisions for protecting their own personal information.
BlackBerry utilizes the following approaches:
 - 1. **Granular application permissions** that enable consumers to which components of their personal information would be shared with the application. Some examples include:
 - a. Personal data: contacts, calendars, device identifiers
 - b. Personal communications: BlackBerry Messenger, personal email, and text messages
 - c. GPS/location, and;
 - 2. **Intuitive user interface design** so that consumers can readily understand how the privacy settings can be adjusted to protect specific components of their personal information.
- 2) **BlackBerry’s third-party application analysis** – To help identify potentially security and privacy-infringing apps, BlackBerry uses its own proprietary program, BlackBerry® Guardian. This program implements a combination of automated and manual analysis to scan apps made available in our storefront, before and after submission into BlackBerry® World™. Additionally, BlackBerry Guardian uses Trend Micro’s Mobile App Reputation technology to incorporate an additional layer of protection for all Android apps available in our storefront. If we identify an app that doesn’t meet our security and privacy criteria, we investigate and from time to time removed apps from BlackBerry World.

- 3) **BlackBerry's customer communication channels** – BlackBerry provides customers with transparent communications about malware risks and potential privacy implications from third-party applications by issuing privacy and malware notices. A privacy notice informs BlackBerry customers that an app, or group of related apps, might pose a privacy risk because the information the app accesses or how it uses that information might not be clearly disclosed to the end user by the vendor. The privacy notice provides information about an app's behavior so that customers can make an informed decision about whether to continue to use the app. A malware notice informs BlackBerry customers about a piece of malicious software that could be installed on a customer's device. A malware notice includes information about the malware, mitigations, and how to remove it from the device. Customers can find these updates on the BlackBerry Security Incident Response Team (BBSIRT) website at www.blackberry.com/bbsirt. In addition, updates are also provided on BBSIRT's Twitter handle, @BBSIRT.
- 4) **BlackBerry's work with app developers** – With concerns over malicious and privacy-infringing third-party apps increasing, BlackBerry is proactively developing and evaluating additional measures and techniques to add protection for customers and their data. To discourage privacy-infringing apps, BlackBerry released Guidelines for Personally Identifiable Information in the BlackBerry® World™ storefront that helps clarify what BlackBerry considers to be personal information and provides general guidance on how it should be protected. If these principles are applied, and third-party app developers comply with privacy/data protection legislation, they will not only help protect customers' personally identifiable information (PII), but also help ensure their apps can remain listed in BlackBerry World. In addition, BlackBerry World provides app developers guidance to help improve the quality, reliability and security of apps submitted to our storefront.
- 5) **BlackBerry's anti-malware and privacy team** - The team responsible for both anti-malware (and privacy) operations and engineering is embedded within the BlackBerry Security Incident Response Team. This integration allows potential malware and privacy issues to be identified, investigated, analyzed and addressed by a group dedicated to improving efficiency and ensuring customers are protected from emerging security issues and privacy concerns.

Given the complex nature and diversity of apps, it is implausible that any mobile vendor will be able to catch 100 percent of all malicious software. This challenge is why BlackBerry has attempted to implement additional layers of security controls to facilitate security and privacy. To that end, BlackBerry's detection capabilities are constantly evolving and adapting to address emerging security and privacy concerns.

- ***Have particular design approaches proven more or less effective than others in protecting consumer privacy and security?***

We believe a comprehensive approach to security and privacy provides the most effective level of protection for customers. By implementing multiple layers of protections, (as previously discussed) and routinely advancing our technology capabilities, we help facilitate customers' ability to keep their data safer from the evolving threat landscape.

- ***What, if any, are the trade-offs between different approaches to providing developers with access to consumers' personal information or device resources?***

In order to find an optimal balance between innovative applications and user privacy, BlackBerry empowers customers to make decisions about whether to allow an application to access a variety of data or device functionality through BlackBerry's granular application permissions. Additionally, BlackBerry's guidance to app developers helps to clarify what BlackBerry considers to be personal information and provides general guidance on how it should be protected. These design features and developer guidance, help to reduce the trade-offs between application innovation and privacy, in a manner that facilitates consumer choice.

II. Secure Distribution Channels

- ***What role should platforms play in creating secure distribution channels, such as app stores, for mobile applications?***

In order to help protect themselves from malware and other types of security concerns, users should avoid downloading and installing applications from untrusted sources, where it is unknown whether there has been any level of app vetting. By taking simple precautionary measures, such as only downloading apps from trusted sources, customers help mitigate the risk of potentially installing malware on their device. At BlackBerry, we're celebrating our fifth anniversary of the BlackBerry World storefront. Today, the BlackBerry World storefront is available in 177 countries – serving BlackBerry customers across the globe. Since the start we have focused on quality – every app goes through a vetting process and as we continue to grow our app offering for our customers, BlackBerry World remains a primary source for applications, and the only way for developers to tap into BlackBerry payment services.

- ***Is application review and testing scalable given the explosive growth of mobile applications? What techniques have proven effective in detecting malicious or privacy-infringing applications?***

Platform security and automated app analysis squeeze attackers from two sides so that the fraction of malicious apps is presently manageable given our expected application release rates. Please see our previous responses about BlackBerry's third-party application analysis and platform security efforts.

- ***Do smaller players in the mobile ecosystem, such as third-party app stores, have the resources to deploy such techniques?***

It depends on the third-party app store, its capabilities, its choices of technologies and partners.

- ***Does limiting application distribution to a single channel provide substantial security benefits? What, if any, are the trade-offs of this approach?***

There are security advantages to limiting application distribution to a single channel, including a definitive control point for application redlisting and well as a forced channel for consistent application security and privacy review. However, by making this restriction, consumer utility and choice may be limited, which should be weighed against any potential additional risks that may come from using a distributed application model. Furthermore, there are effective security techniques that can be leveraged to reduce these risks so that they are similar to a single channel model.

It is important to emphasize that our experience indicates that customers should avoid downloading and installing applications from untrusted sources to help protect themselves from malware and other types of security concerns. By taking simple precautionary measures, such as only downloading apps from trusted sources, customers help mitigate the risk of potentially installing malware on their device.

- ***What are potential alternative approaches to detecting or impeding malicious or privacy-infringing applications on end-user devices?***

As outlined in our response in section “Secure Platform Design”, BlackBerry believes that the most effective approach to mitigating privacy infringing apps and malware is two-fold: first, helping to prevent malicious apps from ever reaching the device by identifying and removing them from the single distribution point; second, leveraging a security hardened mobile operating system with granular app permissions to mitigate privacy risks if a malicious app were to somehow get installed.

For the first component above (single distribution point malware scanning and removal) some companies use an automated-only evaluation approach, while others use a manual app vetting approach. BlackBerry uses a hybrid approach that incorporates both methods, along with proprietary techniques.

For the second component above, instead of focusing on hardening the mobile operating system, some vendors instead rely on reactive, security client applications, such as anti-virus, to help identify and remove installed malicious applications. While this approach is better than nothing, BlackBerry believes that using this strategy alone will fail to keep up with the latest and most sophisticated threats. This approach also consumes device resources, including

battery life, processing power, and bandwidth, thereby negatively impacting the user experience.

III. Secure Development Practices

- ***What resources (e.g., application programming interfaces, development guides, testing tools, etc.) are available for third-party developers interested in secure application development?***

With concerns over malicious and privacy-infringing third-party apps increasing, BlackBerry is proactively developing and evaluating additional measures and techniques to provide additional protection for customers and their data. To discourage privacy-infringing apps, BlackBerry released Guidelines for Personally Identifiable Information in the BlackBerry® World™ storefront that helps clarify what BlackBerry considers personal information and provides general guidance on how it should be protected. This guidance is complemented with training or informational resources that are available to all BlackBerry developers on-line for free, and includes webinars, documentation, as well as up-to-the-minute blogs on specific security and privacy topics. BlackBerry also encourages developers to follow best practices for secure code development, also available through on-line training materials, because good security practices build a solid foundation for privacy. In addition, the BlackBerry app platform leverages security APIs that make security and privacy easier and more effective for the developers (as an example, the BlackBerry Service API for managing customer credentials). If these principles are applied, third-party app developers will not only help protect customers' personally identifiable information (PII), but also enable their apps to remain listed in BlackBerry World. In addition to security and privacy training and guidance, BlackBerry World also provides app developers with guidance to help improve the overall quality and reliability apps submitted to our storefront.

- ***Is the developer community taking advantage of these resources? Are they making common security mistakes?***

Informal analysis indicates that BlackBerry developers do indeed leverage the above resources. BlackBerry web analytical tools provide insight into which resources and documentation are visited, so if important information is not getting enough visibility, the BlackBerry web team can reposition the material. Furthermore, our BlackBerry app development support team holds regular field events with the developer community whereby feedback on developer activities and practices are collected and used to focus training material on key areas that may not be getting enough attention.

- ***Do consumers have the information they need to evaluate the security of an application? Are they aware of potential security risks (e.g., the insecure transmission of data)? Are there ways to make the security of applications more transparent to the end-user?***

BlackBerry attempts to facilitate additional confidence in applications obtained through BlackBerry World through a variety of techniques leveraged by the BlackBerry storefront as discussed in a previous section. Complementing these safeguards is a privacy design strategy that leverages application permissions on the device that readily enable consumers to choose whether they are comfortable to share information with the intended application. These application permissions are granular and transparent with what personal information would be disclosed with the application.

- ***What more can platforms and other industry players do to ensure that third-party developers have the resources and incentives necessary to implement secure development practices?***

As outlined in a previous section, BlackBerry makes educational and training materials available to its developer community about security and privacy best practices, including specific current issues. Many of these security and privacy best practices are platform agnostic, which means that there is a possible opportunity for government or other stakeholder organizations to help raise general security and privacy awareness for the developer community as a whole, encouraging developers to consult the platform vendor of choice for further resources and information.