Project Proposal
Investigating security in BlackBerry Messenger

Cedric van Bockhaven, Peter van Bolhuis,
Connor Dillon, Andy Ptasinski

November 21, 2013

1 Research Questions

• Can we find any security flaws in the implementation of RIM’s BBM on Android phones?
• How secure is BBM on Android compared to WhatsApp and the original BBM on BlackBerry?

2 Project Goals

• Find errors in the implementation of cryptography in the BBM app.
• Determine if there are any backdoors in the BBM app.
• Construct attack plans to exploit the vulnerabilities found.
• Propose solutions to the found vulnerabilities.
• Find out if privacy sensitive information is sent from the phone to the BlackBerry (or other) servers. Examples of privacy sensitive data in this context can be (but are not limited to) the address book and location.
• If time permits: compare the security BBM on Android with WhatsApp and the original BBM on BlackBerry.

3 Significance of the Project

The original BBM communication was well encrypted and did not have any publicly known backdoors. There have been recent revelations of the security vulnerabilities in WhatsApp [1] and information about NSA pressuring vendors into installing backdoors into their systems. This project tries to assess how secure BBM for Android is
compared to its original format as well as its main competitor, and check if there are any possible backdoors that could have been implemented in the app.

4 Project Design

We will analyze network traffic of BBM to try to find possible vectors of attack and to determine if any privacy sensitive information is being leaked from the app.

By default, the BlackBerry version of BBM uses a global PIN encryption key to encrypt messages sent by BBM. This key is installed on all BlackBerry devices so any device can decrypt any message sent by other Blackberry devices. But is is also possible to install an own encryption key and share it with other people [2]. We will evaluate how this is implemented in the Android version of the app.

We will decompile the Dalvik bytecode using tools like Androguard which can decompile the bytecode to fairly readable Java code. The Java code will be analyzed for vulnerabilities and possible backdoors. Recent research shows that is it possible to find errors in cryptography in Dalvik Bytecode through static analysis [3] [4]. We will follow the methods described in these papers to do the same for the BBM app. If any errors are found during the static analysis, we will do practical tests to confirm the problem. If we find security errors in the app, we will propose solutions and do a responsible disclosure.

When our analysis is complete and there is time, the results will be compared to research on the original BlackBerry Messenger.

5 Anticipated Results

RIM has a good track record when it comes to security of their applications, therefore it seems unlikely that there are any major flaws. However, Android is a very different platform than BlackBerry, it's possible RIM has made some mistakes on a platform they are not experienced with. Many of the popular apps in the play store have glaring security vulnerabilities in their implementation as demonstrated in [3] and [4]. If there are any errors, we expect that we will be able to detect them using a combination of static analysis of the decompiled code and practical security testing.
6 Division of Work

The work will roughly be divided as shown in table 1 below.

<table>
<thead>
<tr>
<th>Week</th>
<th>Task</th>
<th>Person(s)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Preparation, reading in, setting up tools</td>
<td>Andy, Cedric, Connor, Peter</td>
</tr>
<tr>
<td>2</td>
<td>Analyse network traffic for wrong certificates and valid for wrong domain. Decompile code and get familiar with code.</td>
<td>Andy, Peter</td>
</tr>
<tr>
<td>3</td>
<td>Use valid certificate check contents of encrypted tunnel. Compare to original BlackBerry Messenger. Check interesting parts of code and more thorough analysis, trying to identify security holes</td>
<td>Cedric, Connor</td>
</tr>
<tr>
<td>4</td>
<td>Making the paper, preparing for presentation</td>
<td>Andy, Cedric, Connor, Peter</td>
</tr>
</tbody>
</table>

References

   https://blog.thijsalkema.de/blog/2013/10/08/piercing-through-whatsapp-s-encryption/


   https://www.owasp.org/images/7/77/Hunting_Down_Broken_SSL_in_Android_Apps_-_Sascha_Fahl\%2BMarian_Harbach\%2BMathew_Smith.pdf


   https://code.google.com/p/androguard/
This project proposal is written in the context of a contractor placing a bid with a company that has indicated that they need a project completed. There could be a number of factors at play here. Others may be bidding against the contractor or an informal opportunity may have arisen based on the relationship between the contractor and the company that requires the project. Regardless, it is important to keep those contextual factors in mind when putting together your project proposal. Project Proposal Template.