Viber Communication Security

Project Proposal

Michiel Appelman (michiel.appelman@os3.nl)
Jeffrey Bosma (jeffrey.bosma@os3.nl)
Gerrie Veerman (gerrie.veerman@os3.nl)

November 17, 2011

Abstract

In the past couple of years more and more communications which used to use the regular mobile operator networks started moving towards IP-based networks. This has given rise to 'apps' on smartphones that enable consumers to connect to each other without the use of their mobile operator. More recently the security implications of switching from the closed network of the operator to the open Internet have become apparent after some apps have shown severe weaknesses. In this project we will take a look at one 'app' in particular: *Viber*, a VoIP application used on cellphones. The research will be carried out during the Security of Systems and Networks (SSN) course at the SNE-master and give an answer to the question how *Viber* performs — security-wise — in comparison to other services.

Contents

1 Introduction

Viber is a communication application for mobile phones. The current version works on Android and iPhone. You are able to call, send text messages, photos or your current Global Position System (GPS) location. It's comparable to other communication apps in this market like *WhatsApp* and *Skype*. Reviews predict this can be a real competitor to Skype, this because of the simplicity that *Viber* offers. Besides this it is free of charge. *Viber* states to be 'freemium' which means offering free services with one app and having a paid app with more attributes/possibilities. Since it is a relative new application we would like to see which ways of security implementations *Viber* has made. This since privacy/security is an important issue regarding communication. A main research question can be formulated in addition with some sub-questions. Within the sub-questions we can look at two sides: Whats actually stored on the phone? What is actually transmitted through the wire? On first sight we couldn't find much information about the security *Viber* offers. In Chapter 2 some references can be found regarding to this.

1.1 Research Questions

Main research question:

> *How secure is communication through the* Viber *application in comparison to other VoIP services?*

Sub-questions about information stored locally:

- What information is stored by *Viber*, and in what form?
- How does *Viber* for iPhone differ from the implementation on Android?
- Are *Viber* messages stored encrypted/scrambled? If yes, what kind of encryption is used? How prone is it to currently known attacks? What about photos, and transmitted location information?

Sub-questions about data transferred over the wire:

- How are *Viber* messages send, are they encrypted/scrambled?
- Can one modify the content, the recipient address, or the sender address of a message?
- What other kind of flaws are present in the protocol, and how can they be improved?

2 Research

Virtually no research has been done in the fields *Viber*'s security. An extensive search on the Internet resulted in only a few vague statements from a spokesperson of *Viber*. This intrigued us and made us very skeptical because the amount of information, the openness about security implementation and the clarity on matters of the spokesperson stating these claims is very dubious to say the least.

The findings about the security implementations in *Viber*, or there absence, are quoted below.

Regarding the personal information collected by *Viber*, we found the following in their privay policy:

> *We take reasonable precaution to protect Personal Information from misuse, loss and unauthorized access. Although we cannot guarantee that Personal Information will not be subject to unauthorized access, we have physical, electronic, and procedural safeguards in place to protect Personal Information. Personal Information is stored on our servers and protected by secured networks to which access is limited to a few authorized employees and personnel. However, no method of transmission over the Internet, or method of electronic storage, is 100% secure.*[1]

Talmon Marco is an online spokesperson for *Viber* and answered a few questions asked by consumers. About encryption of messages he replied as follows:

> *They were not in the very first version, but they are now.* [2]

When asked about the encryption of calls:

> *To be honest, since our code is not open source, we cannot claim 'encryption' as it is not open to outside scrutiny. The most we can say is that 'it is scrambled' (and in our opinion the same applies to anybody who does not have an open source technology).*
>
> *So, Viber messages are scrambled.*[3]

And:

[1] http://viber.com/privacypolicy.html
[2] http://www.quora.com/Talmon-Marco-Are-the-messages-sent-between-Viber-users-encrypted
[3] http://i.tuaw.com/2011/04/01/viber-for-iphone-updated-with-free-text-messaging

> *Like the great majority of major, public VoIP services out there, we don't encrypt our calls, but we do transmit them peer-to-peer (the voice itself never reaches our servers). Viber text messages, however, are encrypted.*[4]

And even went on to say that none of their competitors do either:

> *About encryption – no, the call is not encrypted. none of the free VoIP providers today (including Skype) encrypts calls.* [5]

But as another user noted, Skype had a very nice analysis about their security in 2005:

> *Thanks for your response. It'd be nice if you could provide at least some details of how you're 'scrambling' messages. I for one would also place a lot of value on some 'independent' security analysis, like Tom Berson's analysis that Skype commissioned in 2005* [6]*. I certainly appreciate that you don't want to open your code to the public, and that you don't want to make claims that you cannot back up without opening that code, but I certainly hope you take the issue seriously and take any steps you can to make your product's security more transparent to users.*[7]

2.1 Test Setup

Using a Wireless access point we are going to connect to the Internet through a hub. We connect the hub to a laptop on which we will run WireShark/tcpdump to collect packets transmitted through the network. There are already an Android and two iOS phones available for testing *Viber*.

2.2 Analysis

When we find the data stream send out by *Viber* we will try to decrypt/unscramble it by using basic cryptanalysis tools and techniques. It maybe that our experience in this field is too limited but we will try to discover as much as possible about the protocol they use.

[4] http://www.androidpolice.com/2011/07/20/viber-for-android-leaves-private-beta-now-available-for-e
[5] http://veryrite.com/2010/12/05/viber-makes-free-voip-calls-from-iphone-3g3gs4-ipod-touch-ipad-on-
[6] http://www.intelligentzia.ch/inforum/skype_security_evaluation.pdf
[7] http://i.tuaw.com/2011/04/01/viber-for-iphone-updated-with-free-text-messaging

3 Schedule

3.1 Tasks

We divided the different tasks as follows:

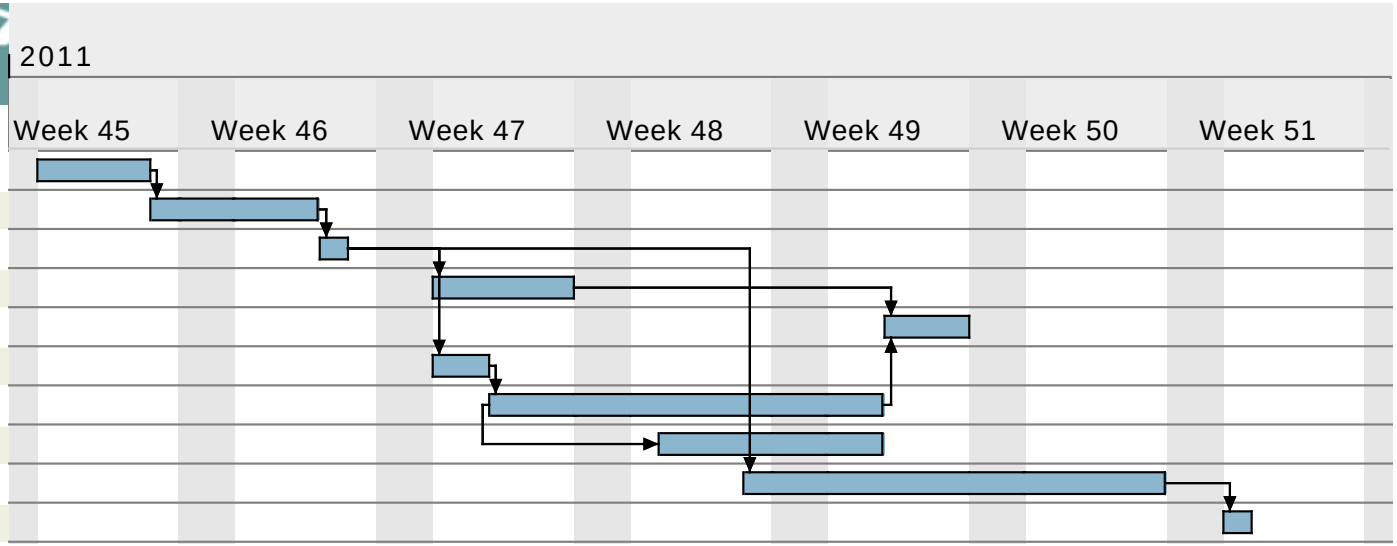
	Gerrie	Jeffrey	Michiel
Project Proposal	✓	✓	✓
Set-up Lab		✓	✓
Research other VoIP Services	✓		
Testing – Local Storage		✓	
Testing – Message Exchange	✓		
Testing – Voice Communication			✓
Compare Services – Skype	✓	✓	
Compare Services – Standard SIP		✓	✓
Write Report	✓	✓	✓
Presentation	✓		✓

3.2 Time Schedule

See page 5.

Gantt Chart

Name	Begin date	
Form a Group	7-11-11	10-11-11
Find a Subject	11-11-11	16-11-11
Make a Project Proposal	17-11-11	17-11-11
Research common VoIP S...	21-11-11	25-11-11
Compare to Viber	7-12-11	9-12-11
Set-up a Test Environment	21-11-11	22-11-11
Test Viber in Lab	23-11-11	6-12-11
Document Weaknesses	29-11-11	6-12-11
Write Report	2-12-11	16-12-11
Presentation	19-12-11	19-12-11



A Group

A.1 Group Members

Michiel Appelman (`michiel.appelman@os3.nl`)
Skills: Networking and scripting.

Jeffrey Bosma (`jeffrey.bosma@os3.nl`)
Skills: Basic Assembly and chip programming skills.

Gerrie Veerman (`gerrie.veerman@os3.nl`)
Skills: All-round engineer.

A.2 Coördination

We keep contact during the classes we have and also e-mail. Apart from IRC we also started using Facebook for IM'ing, which worked surprisingly well.

A.2.1 Repository

Using the Dropbox[8] service we share a common repository of files which we can all use and also has version control integrated. We divided the LaTeX source in different files to edit these separately.

[8] http://www.dropbox.com

B Acronyms

GNU GNU's Not Unix

IM Instant Message

SSN Security of Systems and Networks

SNE Systems and Network Engineering

IP Internet Protocol

IRC Internet Relay Chat

VoIP Voice over IP

SIP Session Initiation Protocol

RTP Real Time Protocol

GPS Global Position System