Security Analysis of Instant Messenger TorChat Master's thesis

Rain Viigipuu

Supervisor: Alexander Norta, PhD External Supervisor: Arnis Paršovs, MSc

June 4, 2015

Challenge

Secure and private communication over the Internet

- Confidentiality
- Integrity
- Authenticity
- Metadata privacy

How to achieve that?





× - c	TorChat: j	2ko25d2vxx	bvz6p
🐣 j2ko2	25d2vxxbvz6p	(myself)	
			_
😣 Add new	contact		
TorChat ID			
Display name			
Introduction	hello, my fri	end	
	Cancel	C)k
_			
			_
	A	h la	
	Availa	DIE	

 j2ko25d2vxxbvz6p (myself) Add new contact TorChat ID nwtuvtf4sidu6mlf Display name friend
Add new contact TorChat ID nwtuvtf4sidu6mlf Display name friend
Add new contact TorChat ID nwtuvtf4sidu6mlf Display name friend
Add new contact TorChat ID nwtuvtf4sidu6mlf Display name friend
TorChat ID nwtuvtf4sidu6mlf Display name friend
Display name friend
Introduction hello, my friend
Cancel Ok
Available

 TorChat: j2ko25d2vxxbvz6p j2ko25d2vxxbvz6p (myself) nwtuvtf4sidu6mlf (friend)
😕 🗇 💷 nwtuvtf4sidu6mlf (friend) j2ko25d2vxxbvz6p
(15:22:02) myself: Hello my friend! (15:22:14) friend: Hello
Available

Objectives

- 1. Document TorChat protocol
- 2. Analyze security of the protocol
- 3. Audit reference implementation

TorChat protocol



Methodology

Based on EFF's "Secure Messaging Scorecard".

- 1. How is the communication protected in transit?
- 2. Can the service be used anonymously?
- 3. Who can learn about communication taking place?
- 4. How user's profile information is protected?
- 5. What forensic evidence is left on the user's device?
- 6. Is the source code available, is software available from trusted source?

Findings (1)

Communication confirmation attack:



Findings (2)

Contact list manipulation:

- Leaks profile information
- Contact confusion attack



Findings (3)

Denial-of-service attacks:

- No limits for message length
 - The command is buffered in memory
 - No limit for chat message
- Filetransfers accepted automatically

		1		_							10 12.01 1	
× - = 00.0% - testfile.bin		× - = 00.0% - testfile.bin		x - 0 (C × - 0 00.09		e.bin		x = 0 00.0% (tes	tfile.bia		
Receiving testfile.bin from c357hifa/im5zmj4f D0.0% (0 of 21 bytes)		Receiving testfile.bin from c357hdfavinSzmj4f 00.0% (0 of 21 bytes)		Receiving te Receiving testfile,bin from c357ht from c357htfa4mSzmj4f 00.0% (0 of : 00.0% (0 of 21 bytes)				Receiving testfile bin from c357h8fa4mSzmj4f 00.0% (0 of 21 bytes)				
Cance	Save as	Cancel	Save as			(Cancel	Save as		Cancel	Save as.	
· · · · · · · · · · · · · · · · · · ·	_	* = 0 00 * = 0 00.0%-test	file.bln		* = 0 00.09	6 - testfil	e.bin		* = 0 00.0%-ter	tfile.bis		
Receiving testfile.bin from c357hdfa4m52mj4f 00.0% (0 of 21 bytes)		Receiving te: Receiving testfile.bin from c357h6 from c357h6fa4m52nji 00.0% (0 of 2 00.0% (0 of 21 bytes)	el .		Receiving testfil from c357h6fa4 00.0% (0 of 21 b	le.bin Im5zmj4f Iytes)			Receiving testfile.bin from c357h6fa4m5zn 00.0% (0 of 21 bytes)	ij4f		
Cance	Save as		Cancel	Save as		. (Cancel	Seve as		Cancel	Save as	
× = 0 00.0% - testfile.bin	_	* × 0.0% - Receiv	ing testfile bin		_	x = 0	00.0% - t	estfile.bin	-tes			
Receiving testfile bin from c357h6fa4m5zmj4f 00.0% (0 of 21 bytes)		Receiving Receiving testfile.b from c357 from c357h6fa4m5 00.0% (0 c 00.0% (0 of 21 byte) Receiving testi from c357b6fz 00.0% (0 of 21			g testfile.bi S7h6fa4mSi O of 21 bytes	in zmj4f s)	sbin nSzn Res)	sbin nSzmj4f Resj		
x = 0 00.0% - testfile.bin				Cance	Save as					tfile.bis		
Receiving testfile, bin from (357hdfa4m5zm)4f 00.0% (0 of 21 bytes)		• = 0 00.0% - testfile.bin			_			Cance	Receiving testfile bin			
		Receiving testfile bin from (357hsfa4m52mj4f 00.0% (0 of 21 bytes)		ajat		sbin nSamj4f		from c357h6fa4m5zmj4f 00.0% (0 of 21 bytes)				
Cance	Save as			Cance	Save as	(tes)		1		Cancel	Save as	
Receiving testfile bin from c357bdf#4m5zmj4f 00.0% (0 of 21 bytes)		Carcel 00.0% (0 of 21 bytes)	Save as	we as	eceiving test/lie.t rom c357htfa4m 0.0% (0 of 21 byte	bin Szmj4f es)		to Th St	Receiving test/fie.blm from c357h6fa4m5zn 00.0% (0 of 21 bytes)	ijat		
* = 0 00.0% - te	estfile.bin	× = 0 00.0% - test	file.bin			in		yve as	* = 0 00.0%-ter	tfile.bin		
Receiving ter from c357hd from c357hdfa4m5a 00.0% (0 of 2 00.0% (0 of 21 bytes	n mj4f i)	Receiving testfile bin from c357hdfa4m5zmj 00.0% (0 of 21 bytes)	e -	Receiving t from c357f 00.0% (0 of	stfile.bin dfø4m5zmj4f 21 bytes)				Receiving testfile bin from c357hdfa4m5zn 00.0% (0 of 21 bytes)	ijat		
	Cancel	Save as	Cancel		c	ancel	Save as	Save as		Cancel	Save as.	

Conclusion

- TorChat design is sound
- TorChat implementation has flaws
- The flaws can be easily fixed

Thank you!

Questions?