An Empirical Survey on how Much Security and Privacy Customers Want in Instant Messengers

Thomas Paul

Munich University of Applied Sciences
Lothstrasse 64, Munich, Germany
e-mail: thomas.paul91@gmail.com

Hans-Joachim Hof
MuSe – Munich IT Security Research Group
Munich University of Applied Sciences
Lothstraße 64, Munich, Germany
e-mail: hof@hm.edu

Abstract— **Instant messengers are popular communication tools used by many people for everyday communication, as well as for work related communication. Following the disclosure of a massive surveillance system by Edward Snowden, many users became aware of the risks of unsecure communication. Users increasingly ask for secure communication. However, unsecure instant messengers are still popular nowadays. This could be due to the fact, that, besides the large number of available instant messengers, no instant messenger fully satisfies the users preferences. To research the acceptance of security mechanisms in instant messengers, this paper presents an evaluation of user preferences for secure instant messengers. A user survey was conducted to rate the acceptance of security mechanisms typically used by instant messengers. The survey clearly shows that users ask for security functionality. The paper presents the features of an ideal instant messenger that fulfills all the user preferences identified by the survey. A market simulation shows that the ideal instant messenger has a high potential for commercial success.**

Keywords-Instant Messaging; instant messenger; security; usability.

I. INTRODUCTION

Today, instant messengers like WhatsApp are important for communication between people, even outrunning the once popular SMS (Short Message Service) [8]. Instant messengers are communication clients for instant messaging networks. Instant messaging networks provide a service called instant messaging that allows transmitting real-time text messages to other users or groups of users. Most instant messaging networks allow users to also transmit pictures or arbitrary files. Following the disclosure of Edward Snowden, secure communication became popular in the press, as well as in user preferences. However, current instant messenger usage does not show a signification shift from unsecure instant messengers to secure instant messengers. This could be due to the fact that none of the existing secure instant messenger fulfills the preferences of the now security-aware users. To fill this gap, the work presented in this paper analyzes user preferences for secure instant messengers. A user survey was conducted to rate the acceptance of security mechanisms typically used by instant messengers. The results of the survey should help developers of future instant messengers to decide on security features to implement.

This paper is structured as follows: Section II discusses related work. Section III presents the design of the user survey. Section IV discusses in detail the findings of the user survey. Section V presents the features of an ideal instant messenger fulfilling all the user preferences identified by the survey. A market simulation is used to show the potential of this ideal instant messenger. Section VI summarizes the findings of the paper.

II. RELATED WORK

There are several studies on instant messenger usage, e.g., [8][11][12][13]. In [8], the popularity of SMS and instant messengers is analyzed. The authors of [11] research how the usage of WhatsApp differs from the usage of SMS. The authors of [12] present a study on how users use instant messaging in building and maintaining social relationships. In [13], the motivation of users for switching instant messengers is discussed. However, most studies focus on one distinct instant messenger and the usage of instant messaging. They do not focus on security preferences of users. Analyzing not only one but several instant messengers helps to identify the features most asked for by users in each messenger. When planning future instant messengers, this knowledge could help to increase the focus on the intended users.

Other publications, e.g., [9][10], have a focus on security, but they analyze only existing security features of instant messengers and attacks on these instant messengers. In [9], security features of instant messengers and attacks on instant messaging are presented. The authors of [10] focus only on attacks on instant messaging. User preferences for secure instant messaging are out of scope of these papers.

In contrast, the user survey presented in this paper focuses on preferences of users regarding security- and privacy-related features of instant messengers. The results of this paper are intended to give a hint on the ideal combination of features that should be included when implementing future instant messengers. The focus of this paper is on stand-alone instant messengers, instant messaging in social messaging platforms is not considered.

ISBN: 978-1-61208-493-0

III. Survey Design

The survey consists of four parts:

1. Socio-demographic questions.
2. General questions about instant messaging.
3. Security-related questions.
4. Choice Based Conjoint Analysis.

Each part of the survey is discussed in detail in the following subsections.

A. *Demographic Questions*

The demographic questions include the typical questions about age and sex. Age groups where: <18, 18-24, 25-29, 30-39,40-49,50-59, 60+.

B. *General Questions About Instant Messaging*

This part of the survey analyzes the degree of brand awareness and usage of popular instant messenger networks. The instant messengers considered in the user survey presented in this paper can be divided into two major groups:

- Instant messengers without focus on security: Facebook Messenger, Hangouts, Hike, Kakao Talk.Kik, Line, Skype, Snapchat, Tango, Viber, and WhatsApp.
- Security-conscious instant messengers with end-to-end encryption: ChatSecure, iMessage, myEnigma, SIMSme, surespot, Telegram, TextSecure, Threema, and Wire.

The list with security-conscious instant messengers shows that there are already several secure alternatives for instant messaging. It is an interesting question if people are using these messengers and if not, why not?

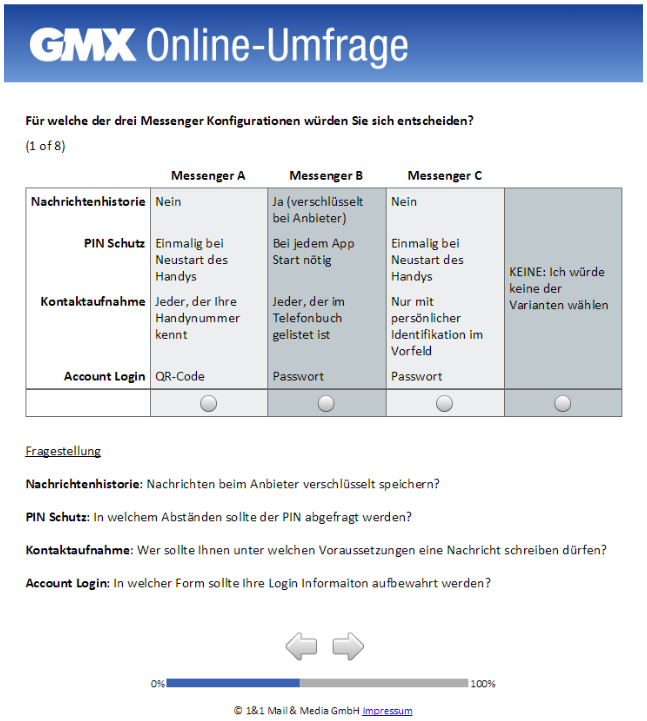
C. *Security-related Questions*

In this section of the survey, participants are asked about their preferences for security features. The list of security features consists of the security features present in the security-conscious instant messengers (ChatSecure, iMessage, myEnigma, SIMSme, surespot, Telegram, TextSecure, Threema, and wire). Users can express their preferences on a scale ranging from 1 (unimportant) to 5 (very important).

Topics of the questions in this section of the survey:

- *Importance of transparency of security features*: does the user want to know what is going on concerning security or does he want security to "just happen behind the scenes"? Does users trust software developers and instant messaging network providers or do they want to have the possibility for external audits?
- *Importance of provider and server location*: Is it important for users that instant messaging network providers are based in Europe and use only servers at European locations or do the users not care about server location, even if the servers are located in the USA with its low data privacy protection level?
- *Convenience versus Security*: If security comes at the cost of a more complicated handling of the instant messenger, is this acceptable for users?
- *Trust in chat partners*: Do users prefer to have control over the content they send to their chat partners?

D. *Choice Based Conjoint Analysis*



GMX Online-Umfrage

Für welche der drei Messenger Konfigurationen würden Sie sich entscheiden?

(1 of 8)

	Messenger A	**Messenger B**	**Messenger C**	
Nachrichtenhistorie	Nein	Ja (verschlüsselt bei Anbieter)	Nein	KEINE: Ich würde keine der Varianten wählen
PIN Schutz	Einmalig bei Neustart des Handys	Bei jedem App Start nötig	Einmalig bei Neustart des Handys	
Kontaktaufnahme	Jeder, der Ihre Handynummer kennt	Jeder, der im Telefonbuch gelistet ist	Nur mit persönlicher Identifikation im Vorfeld	
Account Login	QR-Code	Passwort	Passwort	
	○	○	○	○

Fragestellung

Nachrichtenhistorie: Nachrichten beim Anbieter verschlüsselt speichern?

PIN Schutz: In welchem Abständen sollte der PIN abgefragt werden?

Kontaktaufnahme: Wer sollte Ihnen unter welchen Voraussetzungen eine Nachricht schreiben dürfen?

Account Login: In welcher Form sollte Ihre Login Informaiton aufbewahrt werden?

© 1&1 Mail & Media GmbH Impressum

Figure 1. Example concept selection from the survey

The Choice Based Conjoint Analysis (CBC) [3] is a popular analysis methodology in marketing. CBC is used to survey product preferences of users. CBC can be used to find out, which features or which combination of features users prefer. This section gives a very short introduction into CBC, necessary for understanding of the results of the survey. Please refer to [2] for a thorough discussion of CBC. The core of CBC is to offer customers several concepts of a product and the customer selects the one product concept it likes most (or none). This approach is quite similar to how customers decide on real markets. Hence, the methodology is quite natural for the participants of the survey. The disadvantage of CBC is its inefficiency, resulting in surveys that need a lot of reading of different product concept descriptions by the participants. Figure 1 shows an example of concept choice from the user survey. The question (in German) is: "If you have to chose one of these instant messengers, which would you take?". Concepts are described by attributes. Attributes have two or more levels. For example, if a concept includes an attribute "price", levels may be "1.99 €", "2.50€", and "2.98 €". For the survey presented in this paper, concepts are instant messengers with different features (= attribute levels). CBC

Copyright (c) IARIA, 2016. ISBN: 978-1-61208-493-0

is only suitable for concepts that need a small number of attributes for description, [4] suggests having a maximum of six attributes. Hence, the selection of security- or privacy-relevant features of an Instant Messenger was restricted to those features that are visible to a user. Security features with little or no user interaction are not considered. Existing Instant Messengers are analyzed to come up with realistic security- or privacy-relevant attributes.

The following attributes were chosen for the survey:

- Message history.
- PIN (Personal identification number) protection of instant messenger.
- Type of contact establishment.
- Type of account login.

These attributes and their levels are described in the following and can be seen in Figure 1.

An instant messenger with a *message history* stores sent and received instant messages on a server. In general, a message history can be stored either on a device or on the servers of the instant messaging network. Storing a message history on servers of the instant messenger network poses a risk for user privacy as the servers may be infiltrated and the message history may be stolen or the instant messaging network provider accesses the message history, e.g., to customize advertisement for users. As users today often use multiple devices and change devices often, it is assumed that only a message history stored on the server of the Instant Messenger network provider is realistic.

Hence, the only levels for attribute message history are

- message history and
- no message history.

A *PIN* can be used to restrict access on an instant messenger. A PIN prevents attackers from getting access to the messenger if an attacker has physical access to the device. Also, a PIN can be used to derive a key for encryption of sensitive information of the instant messenger on the device. However, entering a PIN is a hassle for users, see [6][7] for a discussion of the usability problems of PINs and passwords. Hence, the survey distinguishes PIN usage based on the frequency of the usage (once after restart of device, every time the instant messenger is opened).

The levels for attribute PIN protection are:

- PIN must be entered when opening the instant messenger,
- PIN must be entered once after restart of the instant messenger (typically when device is restarted), and
- No PIN.

Another security relevant feature is how users *establish contact* for the first time. The most secure way of contact establishment is meeting in person and exchanging fingerprints of keys used for communication. For example, the instant messenger Threema uses this approach. However, this approach is time-consuming and may be impossible in some cases. Another approach for contact establishment is to only allow contact establishment to parties that have mutual phone book entries (user A has stored the telephone number of user B in his phone book and user B stored the telephone number of user A in his phone book). This approach assumes that the instant messenger is used on a mobile phone. The disadvantage of this approach is that it requires transferring the phone book of the mobile phone an instant messenger is running on to the instant messaging network. This is a serious privacy issue, as phone books hold much information on the social environment of users. Also, if a phone book is transferred to an instant messaging network, much of the data transferred belongs to users that did not explicitly agree to this transfer. Another approach for contact establishment is to allow everybody that knows the phone number of a user to contact this user. The problem with this approach is that a possibly publically known value (phone number) is considered to be secret.

The levels for attribute contact establishment are:

- Meeting in person.
- Mutual phone book entries.
- Phone number known.

Several instant messengers require an *account login* to protect access to the instant messaging network. Account login can be password based or it can use a QR-code that is scanned by the instant messenger on the device. Entering passwords is considered to be a hassle for users, see [6][7] for a discussion on the user-friendliness of passwords.

Possible levels for attribute account login are:

- Password-based account login
- QR-Code based account login

TABLE I. summarizes attributes and levels used for the survey presented in this paper.

TABLE I. FEATURES AND THEIR CHARACTERISTICS FOR CHOICE-BASED CONJOINT ANALYSIS

Attribute	***Message history***	***PIN protection***	***Contact establishment***	***Account login***
Level	Yes	When opening App	Meeting in person	Password
	No	Once after restart	Mutual phone book entries	QR-Code
		No PIN	Phone number known	

Figure 2 shows an overview of the data analysis of the survey. A utility function is used to calculate the part-worth utility of the different levels of an attribute. A concatenation function is used to calculate the conjoint utility.

Hence,

$$U_p = \psi[f_1(x_{1p}), f_2(x_{2p}), \dots, f_i(x_{ip})] \tag{1}$$

, where U_p is the conjoint utility of product p, Ψ the concatenation function, f_i the utility function of attribute i, and x_{ip} the level of attribute i for product p.

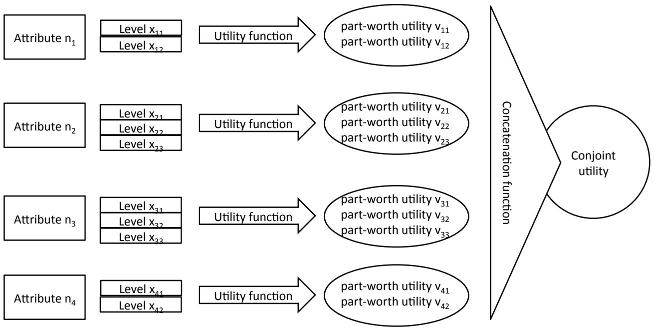


Figure 2. Data analysis

The following utility function is used for this survey:

$$v_{ip} = \sum_{k=1}^{K_i} \beta_{ik} * x_{ikp} \tag{2}$$

, where v_{ip} is the part-worth utility of attribute i for product p, K_i is the total number of levels for attribute i, β_{ik} is the part-worth utility of level k for attribute i, and x_{ikp} is a variable that is 1 if level k of attribute i is present in product p and 0 otherwise.

Concatenation function (3) is used for this survey:

$$U_p = \sum_{i=1}^{I} v_{ip} \tag{3}$$

where U_p is the conjoint utility of product p, v_{ip} is the part-worth net value of attribute i of product p, and I is the total number of attributes.

Inserting (2) in (3) leads to

$$U_p = \sum_{i=1}^{I} \sum_{k=1}^{K_i} \beta_{ik} * x_{ikp} \tag{4}$$

IV. Evaluation of the User Survey

The survey in German language was sent to 200,000 customers of the two participating German freemail providers GMX und Web.de. Hence, it is very likely that most participants of the survey are located in Germany. 1720 users participated in the survey, 640 of them completed the survey. In the following, only the completed survey questionnaires are considered. Participants did not get any incentives for the participation in the survey.

60% of the participants are male, 40% female. 85% of the participants are older then 30 years. The participation in the survey grew with the age of the users. 58% of all participants use instant message clients.

Instant messenger usage varies with age: while nearly all young participants use instant message clients, 64% of the people of age 60 or above do not use instant message clients. This is compliant to the results of [8] that state that older people prefer SMS to instant messengers.

The survey found that the market of instant messengers is dominated by three big players: WhatsApp (81%), Skype (36%), and Facebook Messenger (29%). The figures show that users use more than one instant messenger. This is due to the fact that different instant messengers are used in different social groups a user belongs to. Threema, an instant messenger with focus on security, is only used by 7% of all users. The figures for WhatsApp and Threema are in the same order of magnitude as in a similar study in 2015 about instant messenger distribution in Germany [1].

80% of all participants stated that it is very important or important to have information about the security features of an instant messenger client. This indicates that security is important for users. However, this contrasts to the heavy usage of WhatsApp, an instant messenger with little security features.

52% of participants thought that it is important or very important that the source code of the instant messenger is open source. 24 % thought that it is unimportant or very unimportant to have open source software. These results show that participants distrust the providers of instant messenger software.

70% of participants prefer servers of the instant messenger network to be located only in Europe. Only 8% thought that the location of a server is unimportant. This shows that users are clearly aware of the Internet scale spying activities of several governments. Also, this number shows that users become more and more sensitive to security and privacy issues in communication.

One important security feature is hiding messages from unauthorized access. However, this security requirement clashes with a convenience feature: message preview on the lock screen. Users clearly vote for convenience when asked for a choice between convenience and security: 45% of participants want messages to show on the lock screen in contrast to 29% of participants that considered this feature to be unimportant or very unimportant.

Another security feature popular, e.g., in Snapchat, is to make screen shots impossible such that received messages cannot be recorded. 45% of participants regarded it important that communication partners cannot take screenshots of the instant message conversation. 29% thought that this feature is unimportant or very unimportant. It is interesting that a similar question of the survey gets the opposite result: when asked, if received images should only be visible in the messenger not outside, 42% disagreed, only 34% agreed.

The CBC analysis using the attributes message history, PIN protection, contact establishment, and account login was used to compare different instant messenger concepts, see Section III.D for details on attributes used and their respective levels. The analysis of the importance of the attributes showed, that for the participants, PIN protection and contact establishment are the most important attributes.

The participants prefer to have a PIN protection of the instant messenger, but they want to enter the PIN only once after restart. Again, users decide for a lower level of security if the choice is security or convenience. However, the survey also shows that users consider PIN protection important, hence they decided for a more convenient but less secure instant messenger concept but they did not choose the most unsecure instant messenger concept (no PIN).

The participants prefer to allow only those persons to contact them that are in their phone book. Again, the users ignore privacy issues (transfer of phone book to instant messaging network) if the choice is privacy or convenience.

The participants voted to have a message history in an instant messenger.

The participants prefer to use traditional passwords for account logon. They do not want to use the more convenient login using a QR code. It is assumed that this is the case because users are not used to QR codes.

V. Market Simulation

A market simulation is used to show the potential market shares that an instant messenger that is based on the results of the survey can get. Part-worth utilities from the CBC are used for a market simulation using the Sawtooth Simulator (http://www.sawtoothsoftware.com/). The following concepts of instant messengers are used for the market simulation:

- WhatsApp Configuration: A configuration similar to the popular WhatsApp instant messenger.
- Threema Configuration A: A configuration similar to the secure instant messenger Threema. As Threema offers multiple features, two Threema configurations were used.
- Threema Configuration B: See Threema Configuration A.
- Best Configuration: A configuration using only those features with best part-worth utility.
- Worst Configuration: A configuration using only those features with worst part-worth utility.

See TABLE II. for details of the levels selected for the configurations above.

Figure 3 shows the results of the market simulation: 68% of the customers would choose the best configuration instant messenger. Only 18% respective 16% would vote for Threema B/A, 8,26% for WhatsApp. However, it should be noted, that instant messenger usage follows the network effect [5]. The network effect states that a network is more valuable for a user if it has many participants. Hence, well established Instant Messenger networks like WhatsApp will always be very popular for new users and new messengers have problems getting a critical mass of users. However, the market simulations shows great potential for a new instant messenger designed based on the results of the survey presented in this paper.

TABLE II. WhatsApp Configuration for Market Simulation

Attribute	***Message history***	***PIN protection***	***Contact establishment***	***Account login***
WhatsApp	No	No PIN	Phone number known	Password
Threema A	No	Once after restart	Mutual phone book entries	Password
Threema B	No	When opening App	Meeting in person	QR-Code
Best	Yes	Once after restart	Mutual phone book entries	Password
Worst	No	No PIN	Meeting in person	QR-Code

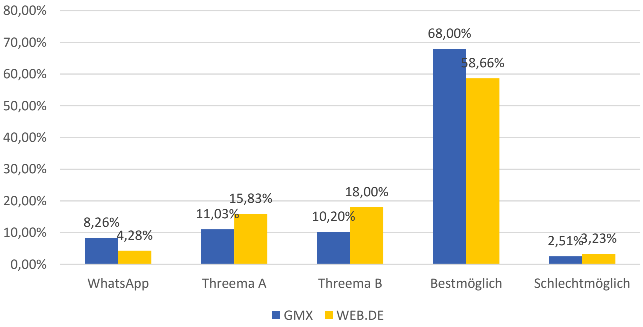


Figure 3. Results of the market simulation

VI. Conclusion

This paper presents the results of a survey on user preferences for instant messengers with a special focus on security and privacy features. The survey holds some interesting insights into user preferences in secure instant messengers, e.g., that instant messenger users have a desire for security and privacy protecting instant messengers. However, they are not willing to accept inconveniences to have a higher level of security. Security features are accepted if they require only little or no user effort. If users have the choice between convenience and security, they decide for convenience. The insights of this paper are suitable for improving the development of secure instant messengers in the future. The most popular unsecure messenger used is WhatsApp, the most popular secure messenger is Threema. However, the survey showed that both messengers do not fit well to the preferences of users. The results of the survey were used to design a new instant messenger with the most promising features. A market simulation shows that this instant messenger has a great potential. If network effects were neglected, this instant messenger would gain 68% of market share in contrast to 8% for a WhatsApp-like instant messenger and 15%-18% for a Threema-like messenger.

ACKNOWLEDGEMENT

The authors want to thank Adrian Klie and the 1&1 Internet SE (part of the United Internet Group) for their support of this work. The survey would not have been possible without their help.

REFERENCES

[1] Deutsches Institut für Vetrauen und Sicherheit im Internet (DIVSI), “Allgemeine Geschäftsbedingungen (AGB) of communication providers” [Online], Available from: https://www.divsi.de/wp-content/uploads/2015/10/2015-10-22_DIVSI_AGB-Umfrage_Charts.pdf, [retrieved: June, 2016].

[2] Swatooth Software Inc., “The CBC System for Choice-Based Conjoint Analysis – Version 8” [Online], Sawtooth Software Technical Paper Series, Available from:

https://sawtoothsoftware.com/download/techpap/cbctech.pdf, [retrieved: June, 2016], February 2013.

[3] J. Louviere and G. G. Woodworth, "Design and Analysis of Simulated Consumer Choice or Allocation Experiments: An Approach Based on Aggregate Data", Journal of Marketing Research , vol. 20, no 4, American Marketing Association, DOI:10.2307/3151440, November 1983, pp. 350-367.

[4] P. E. Green and V. Srinivasan, “Conjoint Analysis in Marketing Research: New Developments and Directions”, Journal of Marketing, vol. 54, no 4, American Marketing Association, DOI: 10.2307/1251756 , October 1990, pp. 3-19.

[5] M. L. Katz and C. Shapiro, “Systems Competition and Network Effects”, The Journal of Economic Perspectives, vol. 8, no. 2, American Economic Association, ISSN 08953309, Spring 1994, pp. 93-115.

[6] H.-J. Hof, “Towards Enhanced Usability of IT Security Mechanisms – How to Design Usable IT Security Mechanisms Using the Example of Email Encryption“, International Journal On Advances in Security, vol. 6, no. 1&2, ISSN 1942-2636, 2013, pp. 78-87.

[7] H.-J. Hof, “User-Centric IT Security – How to Design Usable Security Mechanisms”, The Fifth International Conference on Advances in Human-oriented and Personalized Mechanisms, Technologies, and Services (CENTRIC 2012, 2012), pp. 7-12.

[8] Institut für Demoskopie Allensbach, “WhatsApp on the Rise”, Allensbacher Kurzbericht – 17.01.2014, [Online], Available from: http://www.ifd-allensbach.de/uploads/tx_reportsndocs/PD_2014_01.pdf [retrieved: June, 2016].

[9] M. Mannan and P.C. van Oorschot, “Secure Public Instant Messaging: A Survey”, Proceedings of the 2nd Annual Conference on Privacy, Security and Trust(PST'04), Fredericton, NB, Canada, 2004, pp. 69-77.

[10] N. Leavitt, “Instant messaging: a new target for hackers”, Computer, vol. 38, no. 7, ISSN 0018-9162, 2005, pp. 20-23.

[11] K. Church and R. de Oliveira, “What’s up with whatsapp?: comparing mobile instant messaging behaviors with traditional SMS”, Proceedings of the 15th international conference on Human-computer interaction with mobile devices and services”, ACM New York, ISBN 978-1-4503-2273-7, 2013, pp. 352-361.

[12] W. Wang, J.J. P.-A. Hsieh, and B. Song, “Understanding User Satisfaction With Instant Messaging: An Empirical Survey Study”, International Journal of Human-Computer Interaction, vol. 28, no. 3, 2012, pp. 153-162,

[13] A. C. Y. Hou, “Switching Motivations on Instant Messaging: A Study Based on Two Factor Theory”, Multidisciplinary Social Networks Research, Series Communications in Computer and Information Science, vol. 540, 2015, pp. 3-15.