1 A Secure and Efficient Communication Tool

Matteo Cagnazzo, Patrick Wegner and Norbert Pohlmann

Abstract Communication has changed dramatically in recent years due to the dawn of new ICT technologies and the need of people to communicate in real time. This paper will introduce a little communication theory as a background, compare current technologies and finally introduce a smart, efficient and secure communication platform. It will furthermore address further improvements to the new platform.

1.1 Communication means sharing information

Nowadays information has an unprecedented importance. It has never been easier to share information with other entities. An information is based on characters that are connected via a syntax and grammar to form data. Setting this data into context is information. “Sharing information” creates knowledge and to share information one must communicate. There must be a sender and a receiver who communicate. It surrounds our everyday life more than ever, especially at work. Communication can reach different degrees of efficiency and organized in various ways. Efficiency can be determined by individual skills of participants as well as differences in the established communication structure and culture [1].

Communication can be ranked in terms of relevance. Should this information be accessible by everyone or just a special group of people? Or is there one specified recipient for one specific information. Depending on this classification and the criticality of the transferred information a secured and trustworthy environment may be needed. Technologically speaking this means to establish a trust and security level through end to end encryption or at least transport layer encryption to secure the transmission. Adding such security measures will result in a complex system which can create a trustworthy connectedness of the participating entities.

Corporate communication includes every communication process no matter if it is in- or outbound. This includes the sharing of information between employees as well as communication of the corporation to employees. Through communication an organization gains knowledge and if this knowledge is managed properly an organization can draw strategic decisions from it which gives them competitive advantages. That is why communication is such an integral part of modern businesses [2].

Matteo Cagnazzo
E-Mail: cagnazzo@internet-sicherheit.de

Patrick Wegner
E-Mail: wegner@internet-sicherheit.de

Prof. Dr. Norbert Pohlmann
E-Mail: pohlmann@internet-sicherheit.de

1.2 Digital communication in organization nowadays

Through installed telecommunication systems e.g. mail client, social business network or telephone organizations connect their employees so that they can communicate. Nowadays there is a focus on e-mails through which most of the communication inside of organizations happens, no matter how big or small. Worldwide the number of in- and outbound mails is 116 billion with an upward trend. On average this means that every employee deals with 123 mails per day [3]. The time that is expended daily to answer those mails is not negligible. If every mail is processed for just one minute, an employee is occupied for two hours on average. If it's an executive this number increases and they are spending most of their time at work with communication.

Optimization of such communication habits are already on the rise. Especially mailing is being questioned because of the excessive amount of mails being exchanged on a daily basis and therefore not being too efficient. Even though the decade old system works and is being used by a majority of people it is not capable of dealing with today's technologies.

Mailing is nowadays characterized by formalities formulated personally but they are not meant personal. Repeating salutation and farewell patterns, empty phrases, and disclaimers are generating a significant overhead. The information of a mail can be one sentence but due to the overhead the mail becomes long and extensive. If this mail becomes part of a collaborative exchange because of a document that a group of people is working on it results in poorly structured, swelling and never ending discussions. This offers a possibility to break with norms and structure communication more efficient, smart and modern.

Apart from this way of transmitting information mailing is not capable of dealing with today's security requirements and it is comparatively unsafe to write a mail. It is easy to manipulate whole messages or forge the address of sender or receiver [4] [5].

There are possibilities to protect against such frauds for example end-to-end encryption with "Pretty Good Privacy, PGP" but they are not usable out of the box [6]. Due to the complexity and not usability by non-professionals such solutions to the trust and security problems are not popular. There are ways to secure the transport layer e.g. STARTLS so that the user can be sure no one eavesdrops on their communication but it does not offer security on the different nodes through which a mail is routed [7]. The harm done by digital attacks against companies is estimated at $400 billion a year [8]. This clarifies the need for a suitable secure communication solution. There has to be an exchange of technology which offers new ways to share critical information in businesses.

1.3 New and efficient communication approaches

New and modern approaches help to optimize the communication behavior in organizations and establish a culture of efficient communication. A robust founda-

tion is necessary which is depicted by a modern, forward looking and secure architecture. An efficient, smart and secure communication tool is not a trivial task but it is a very complex challenge not just from a technological point of view. One of the main challenges is to offer the user new and efficient ways of sharing information which are intuitively and easily usable and on the other hand offer a reasonably high security level. Based on these more complex scenarios are implementable e.g. depicting business processes to digitize them and transform businesses.

1.3.1 Transforming old into new

A first step towards an efficient and modern communication technique is already available but the idea behind it is not new. Instant messaging is existent for more than 40 years and gained popularity in the mid 1990's [9]. Programs like ICQ and AOL messenger were the most prominent tools available. They enabled real time communication from sender to receiver no matter how many miles apart [10] [11].

Favored by the increasing popularity of smart phones and social networks instant messaging gained a lot of traction in the past years. The most popular messenger nowadays is WhatsApp with one billion users [12] and over 30 billion exchanged messages a day [13]. Our everyday communication is moving from asynchronous towards a synchronous real time exchange of information.

These change in behavior is especially remarkable for adolescents for who instant messaging becomes an inherent part of their life [14].

Analyzing behavior there is huge increase of pictorial representations (e.g. with emoji's) of expressing feelings instead of describing them textual. Whole phrases can be reduced e.g. "see you" is shortened to "cu ". The transmitted information is the same but "cu" saves 66% of the characters. Especially greeting and farewell phrases are shortened and common phrases like "for your information" – fyi.

There is more to the change in behavior than just the shortening of phrases. The "hashtag" for example is a modern element which gained popularity through micro blogging services. Buzzwords in a message are "hashtagged" (e.g. "#hashtag") and therefore these words become searchable, because they are now tagged. With this tagging language now becomes searchable and this offers new possibilities and dimensions in communication. In a closed system certain messages are easy to find and can be brought in context with other topics and can be categorized and the whole message gets a defined context. Furthermore, it is possible to analyze the relation of hashtags and key performance indicators e.g. "Done with the module #milestone" by the frequency of the hashtag and weighting of it.

The current boom of new techniques and possibilities in communication paired with new mechanics need to be transferred into the business sector right now because those modern and efficient approaches are mapping the needs of corporations to digitize themselves. One question to ask is which requirements should a platform meet to digitalize a business in a holistic way.

1.4 Efficient business tools and security

Meanwhile, there are some systems which are concerned with the transfer of the in 1.3 introduced approaches from the private to the business environment. However, these systems focus mostly on a particular topic. For example, they enable effective communication through the implementation of instant messaging concepts or focus on other specific features, such as document management. Dedicated social networks for internal communication in organizations take an additional step by focusing on relationships between employees. The security subject is treated individually by all available solutions, so that a different number of security features may be included, both from the perspective of the user as well as at technical level.

Instant messaging slowly but surely finds its way into business communication. The popular cloud-based collaboration tool Slack shows this development by its steadily growing number of up to three million daily active users [15]. Slack offers possibilities to communicate with employees in the same organization through different types of channels. Direct messages can be easily exchanged between two persons. In contrast, open channels provide space for group discussions, such as special topics or projects.

The first positive effects can already be observed in using this service. The number of internally sent emails has been reduced by up to 48.5% [16]. Furthermore, an increase in productivity as well as a reduction of necessary meetings can be determined, which additionally confirms the concept and emphasizes the use of new modern, efficient and smart tools in business communication.

When reviewing the security practices of that service, it can be seen that the concept does not include all possibilities to protect the customer's data. While all traffic in transit goes over an encrypted connection, so no one can eavesdrop on it and customer data is encrypted at rest by the service provider on their servers, using the latest recommended secure cipher suites, there is no end-to-end encryption included [17]. Therefore, customers still hand over their data to a third party by sending it to the provider's servers. This approach is followed by several solutions in the business environment. WhatsApp is also a popular instant messaging service which is also establishing end to end encryption but they offer no compliance to business systems so that processes can be integrated. It is solely focused on being a product for customers and not for businesses (s. Table 1.1 **Overview of leading apps in private and business sector**).

Table 1.1 Overview of leading apps in private and business sector

Product	WhatsApp	Dropbox	Slack
Sector	Private	Both	Business

Focused on	Messaging	Document Management	Messaging
Business compliance	No	No	License depending
End-to-end encryption	Yes	No	No
Encryption of data in transit?	Yes	Yes	Yes
Encryption of data at rest?	Yes	Yes	Yes
Provider has access to user data?	Maybe	Yes	Yes
Provider use data for itself?	Yes	Yes	Yes
Users must trust provider?	Yes	Yes	Yes

1.5 Quvert – Smart. Efficient. Secure.

Quvert is a modern and innovative communication tool and enables fast, reliable, usable and secure business communication. It is tailored for daily internal corporate communication with the primary goal to increase the effectiveness without sacrificing security, privacy and usability. These points were considered from the beginning of the planning phase and form parts of the foundation of the platform.

Quvert is chat-based and includes all now well-known advantages of instant messaging, such as sending text messages in real time, exchanging different types of media or using hashtags and similar techniques. However, Quvert does not stop here. In addition to introducing new approaches for transferring information between employees, like the concept for the exchange of internal company knowledge, Quvert also integrates business processes.

The foundation of Quvert is a secure, distributed and reliable server based on XMPP and Erlang with various database-schemes (e.g. Postgres or CouchDB) available to ensure up to 99,99999 % service uptime. The mobile and desktop applications have a composed user interface and are easily usable by non-professionals. They also provide security in terms that user input can be concealed and all messages are encrypted on transport and application layer before they are being transmitted to the server. The encryption scheme is the Signal protocol that has already proven that it is capable of securing connections efficiently also in asynchronous transportations by using ratchets [18]. The whole platform is designed by the following principles:

1. Business by design: Inclusion of business processes into a communication Platform
2. Compliance by design: Data autonomy and legally watertight archiving
3. Security by design: Usable and economic security from the start of development
4. Privacy by design: Privacy is dealt with during the development process to preserve it
5. Usability by design: Easy and usable for users, low training periods

Quvert has no access to user data and does not use it to generate personalized advertisements or feedback. Furthermore, no data is transmitted to third parties and companies can use an on premise server to be sure they do not share any sensible data with the service and everything is kept in house. To be compliant Quvert offers Handshakes where users can define business relevant topics to be archived. If users do not send a specified handshake the server acts as a zero knowledge server. If the handshake is activated the server stores the message in an encrypted database which is only decryptable via four eyes principle to offer legally watertight agreements (s. **Figure 1.1: Handshake flow**

). One side effect of this is that business irrelevant communication is not stored by the service and therefore usage of disk space can be reduced.

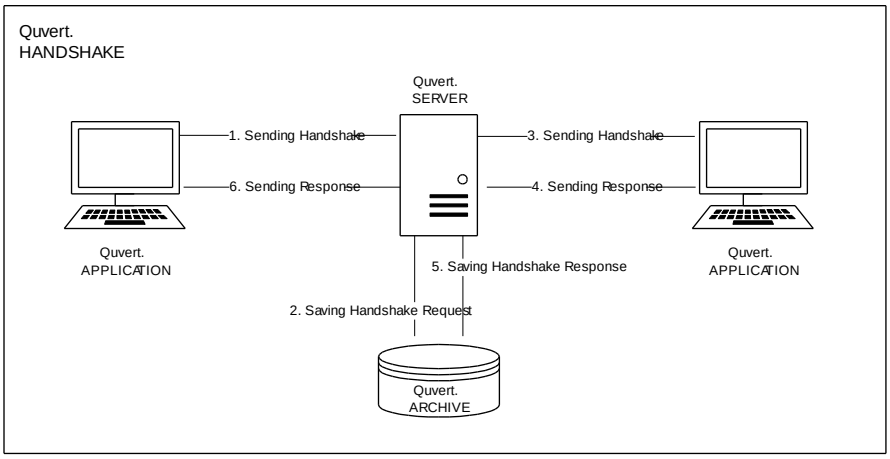

Figure 1.1: Handshake flow

Quvert has a module called Quvert.Knowledge which uses anonymized data to get an overview of the knowledge available in the company and what kind of profile a new employee should have to grant an increase in knowledge available in the organization. This is especially vital in times of demographic change where staff grows older and leaves the company and therefore their knowledge is gone and on the other hand less young people are joining the company [19].

Table 1.2 Quvert in comparison

Product	WhatsApp	Dropbox	Slack	Quvert
Sector	Private	Both	Business	Business
Focused on	Messaging	Document Management	Messaging	Business processes
Business compliance	No	No	License depending	Yes

End-to-end encryption	Yes	No	No	Yes
Encryption of data in transit?	Yes	Yes	Yes	Yes
Encryption of data at rest?	Yes	Yes	Yes	Yes
Provider has access to user data?	Maybe	Yes	Yes	No
Provider use data for it-self?	Yes	Yes	Yes	No
Users must trust provider?	Yes	Yes	Yes	No

1.6 Summary

To create an usable, secure and efficient communication tool is not a trivial task. In terms of security for the platform there has to be a solution to post quantum cryptography and how to modify the Signal protocol to gain the highest possible security. Table 1.2 shows Quvert in comparison to a few of other business communication tools on the market.

Furthermore, it is essential to verify the functionalities offered by Quvert to get to know how the platform is accepted by users. Therefore, testers have been acquired but at the time of writing this paper no results could be drawn from the feedback and this is to be analyzed in the future. There will also be penetration testing in the near future to evaluate possible threat vectors for the platform and to prevent data leakage.

Current research is in the field of Internet of Things to connect Smart Objects to the platform and offer interactive and configurable control panels based on the transmitted certificate attributes by Smart Objects [20].

All in all Quvert shows a promising approach towards a smart, efficient and secure communication platform that is usable on all current operating systems, whether they are mobile or stationary. It also adds real value to currently used communication systems by offering an integrated lightweight yet highly utilizable knowledge management and one can conduct legally watertight agreements. In the near future the connection to the Internet of Things will also serve as a unique identifier for the platform.

References

[1] D. Leonard-Barton, "Wellsprings of knowledge: Building and sustaining the sources of innovation," *University of Illinois at Urbana-Champaign's Academy for Entrepreneurial Leadership Historical Research Reference in Entrepreneurship,* 1995.

[2] R. Thorpe et al. "Using knowledge within small and medium-sized firms: A systematic review of the evidence," *International Journal of Management Reviews,* pp. 257-281, 2005.

[3] The Radicati Group, Inc., "Email Statistics Report, 2015-2019," Palo Alto, CA, USA, 2015.

[4] M. E. J. Newman, S. Forrest and J. Balthrop, "Email networks and the spread of computer viruses," *Phys. Rev. E,* p. 4, 09 2002.

[5] Z. Durumeric, D. Adrian, A. Mirian, J. Kasten, E. Bursztein, N. Lidzborski, K. Thomas, V. Eranti, M. Bailey and J. A. Halderman, "Neither snow nor rain nor mitm...: An empirical analysis of email delivery security," *Proceedings of the 2015 ACM Conference on Internet Measurement Conference,* pp. 27-39, 2015.

[6] P. Zimmermann, "Phil Zimmermann - Why I Wrote PGP," 06 1991. [Online]. Available: https://www.philzimmermann.com/EN/essays/WhyIWrotePGP.html. [Accessed 17 08 2016].

[7] P. Hoffman, "Smtp service extension for secure SMTP over TLS," 1998.

[8] S. Gandel, "Lloyd's CEO: Cyber attacks cost companies $400 billion every year," Fortune, 23 01 2015. [Online]. Available: http://fortune.com/2015/01/23/cyber-attack-insurance-lloyds/. [Accessed 21 10 2016].

[9] T. Van Vleck, "The History of Electronic Mail," 01 02 2001. [Online]. Available: http://www.multicians.org/thvv/mail-history.html. [Accessed 19 08 2016].

[10] ICQ LLC, "ICQ," 1998-2016. [Online]. Available: https://icq.com/. [Accessed 19 08 2016].

[11] AOL Inc., "AIM," 2016. [Online]. Available: https://www.aim.com/. [Accessed 19 08 2016].

[12] WhatsApp Inc., "WhatsApp Blog," 01 02 2016. [Online]. Available: https://blog.whatsapp.com/616/Eine-Milliarde. [Accessed 31 08 2016].

[13] E. Kim, "WhatsApp's Insane Growth Continues: 100 Million New Users in 4 Months," Business Insider INDIA, 07 01 2015. [Online]. Available: http://www.businessinsider.in/WhatsApps-Insane-Growth-Continues-100-

Million-New-Users-in-4-Months/articleshow/45786867.cms. [Accessed 31 08 2016].

[14] J. B. Graham, "Impacts of Text Messaging on Adolescents' Communication Skills: School Social Workers' Perceptions," 2013.

[15] Slack Technologies, "A little update about a lot of people using Slack," 25 05 2016. [Online]. Available: https://slackhq.com/a-little-update-about-a-lot-of-people-using-slack-f16c5b331647. [Accessed 26 08 2016].

[16] Slack Technologies, "How can Slack help my team?," [Online]. Available: https://slack.com/results. [Accessed 26 08 2016].

[17] Slack Technologies, "Slack Policies," 01 12 2015. [Online]. Available: https://slack.com/security-practices. [Accessed 30 08 2016].

[18] T. Frosch and C. e. a. Mainka, "Horst Görtz Institut for IT-Security, Ruhr University Bochum," 2014. [Online]. Available: eprint.iacr.org/2014/904.pdf. [Accessed 31 08 2016].

[19] J. Poterba, "Economic Implications of Demographic Change," *Business Economics,* vol. 51, no. 1, pp. 3-7, 2016.

[20] M. Cagnazzo, M. Hertlein and N. Pohlmann, "An Usable Applicationan for Authentication, Communication and Access Management in the Internet Of Things," *Communications in Computer and Information Science,* 2016.