CryptoCloak application - main idea, an overview and improvement proposal

Dijana Vukovic[1,2], Zoran Djuric[2], Danilo Gligoroski[1]

[1]Department of Telematics, NTNU, O.S. Bragstads plass 2B, Trondheim, Norway

[2]Department of Computer Science and Informatics, Faculty of Electrical Engineering, Patre 5, Banja Luka, Bosnia and Herzegovina

Abstract

Since July 2013, a lot of effort has been invested into spy-resistant application development. "Surveillance" and "privacy" became terms heard more often, both in informal conversations and in security research community. Different initiatives took a place world-wide by Electronic Frontier Foundation and similar organizations to fight for the Internet as it is used to be (e.g. "The day we fight back", "Reset the Net", etc.). Arms race started in the application development, offering different kind of privacy protection for average end-users: anonymous Internet browsing, secret chats, e-mail encryption, etc. CryptoCloak is an application for privacy protected chat communication. Encrypted communication is masked with dynamic cheap chat conversation. In the current version of the CryptoCloak, Diffie-Hellman key exchange is done in clandestine manner - instead of sending uniform sequence of numbers over the network, sentences are sent. It produces huge overhead. In this paper, CryptoCloak tool is introduced and one proposal for its improvement is given.

1 Introduction

Internet surveillance exists for a long time, but people became more aware of it after Snowden affair started[1]. Even average end-users became interesting in the applications provide secure communication and privacy protection. Revelations about NSA partnership with leading companies in the Internet communication have appeared (e.g. Microsoft, Google, Skype, etc.)[2]. The fact that the NSA has an access to the private communication of individuals is a huge violation of privacy. "Surveillance/privacy" issue led to developing tools for anonymous communication over the Internet. There are applications with different purpose, from anonymous Internet browsers to secure communication over instant messengers. Huge set of these applications is available for free.

This paper was presented at the NIK-2014 conference; see http://www.nik.no/.

Second section gives an overview of terms ”surveillance” and ”privacy”. It is important to explain these terms in detail, to highlight the consequences that may occur if these two terms are disrupted. In section 3, related work to CryptoCloak application is discussed, with a short overview of two widely used secure chat applications: Cryptocat and Telegram. In section 4, CryptoCloak application is presented and its major disadvantage is pointed out. In section 5 an improvement for the CryptoCloak application is proposed. Section 6 gives a short note of the further work, and the paper is concluded in Section 7.

2 Surveillance and privacy

In this section an overview of terms ”surveillance” and ”privacy” is given. Well understanding of these terms is required to highlight the consequences that may occur if they are disrupted.

Surveillance can be defined as ”close observation of a person or group, especially one under suspicion”[3]. Law enforcement agencies needed the ability to conduct electronic surveillance with the following goals: crime and terrorism prevention, prevention of any kind of malicious activities exploiting the Internet. To achieve these goals, Internet surveillance has been one of the solutions.

Many people have opposed surveillance because it can be considered as an invasion of privacy (as with hidden video cameras) or a tool of social control (as in monitoring workers). To avoid issues of using surveillance, perpetrators of surveillance use five methods to minimize adverse actions to their actions[3]: cover-up and exposure, devaluation and validation, interpretation struggles, official channels, and intimidation, bribery, and resistance. Individual resistance to surveillance can appear in different shapes: avoiding detection, refusing to provide information, and encouraging surveillance agents not to enforce regulations. Surveillance can be justified in some cases, as a cracking down a crime, or increasing efficiency of service systems, but it can also be a big threat to privacy.

Privacy can simply be defined as ”the right to be left alone”. In the online context, privacy has to include rights of an individual to: be aware of what kind of information is collected about them and how it will be used, have an access to the information held about them and know that it is accurate and safe, to have some degree of anonymity (for example, Web-browsing habits should not be tracked), and to send/receive e-mail messages or other data safely, without a fear that these will be intercepted or read by persons other than the intended recipient(s).

The statement of social networks cofounders (Google and Facebook) ”the age of privacy is over” from 2010 lead to many discussions on that topic over the years. Bruce Schneier in [4] states that privacy is about control, and that people need to be responsible for taking care of their private information in a way that they decides how it will be shared, where it will be shared, and with whom. But what to do nowadays when the Internet surveillance is all around? Even if people think they are controlling their privacy, using e.g. chat applications for secure communication, the fact that the encrypted content will be stored for further analysis make that thoughts questionable. After Snowdans whistle-blower act in 2013, people started more to worry about their privacy, and to fight against NSA surveillance. In July 2013 the ”International Principles on the Application of Human Rights to Communications Surveillance” was published[5]. It gives explanation ”how international human rights law applies in the current digital environment, particularly in light of the increase in and changes to communications surveillance technologies and techniques”. They defined communication surveillance as ”the monitoring, interception, collection, analysis, use, preservation and

retention of, interference with, or access to information that includes, reflects, arises from or is about a persons communications in the past, present or future". The principles are: legality, legitimate aim (surveillance should be permitted only in the case if that is justified legal interests of democratic society), necessity, adequacy, proportionality, competent judicial authority ,due process, user notification (individuals has to know about decisions of authorizing surveillance, and must have the access to the materials that confirms it), transparency, public oversight, integrity of communications and systems, safeguards for international cooperation, and safeguards against illegitimate access - legislation criminalizing illegal communications surveillance by public or private actors has to be enacted.

Privacy is the right of each individual, and it should not be threatened if it is not harmful to the others. These surveillance and privacy issues were the main reason for the information security community to start developing solutions for their solving. The CryptoCloak project started with the same intention.

3 Related work

CryptoCloak is an application for privacy protected chat communication. In this section chat applications similar to the CryptoCloak are presented. The most popular chat applications for anonymous communication over the Internet are: Cryptocat[6] and Telegram[7].

CryptoCat uses a modern web technology to provide an application which is very simple to adopt and ease to use for the average end-user. It is developed as a plug-in for the most popular web browsers. Chat communication is encrypted before sending - even the CryptoCat network itself is not able to read. All cryptographic operations take place on the client side - server is only involved in the exchange of cipher text and user login. To provide conversation privacy, CryptoCat uses OTR (Off-the-Record Messaging protocol).

Telegram messenger is a cross-platform whose clients are open source. Telegram provides to an average end-user: privacy protection (with heavily encrypted messages that can be self-destructed), accessibility to messages from different devices (cloud-based), and secure communication without any limits in the size of chat messages. Besides that, Telegram is free and open application. According to Telegram's "Privacy policy"[8], it does not store secret chat messages, but the phone contacts from application user are stored.

Both CryptoCat and Telegram provides end-to-end encryption. CryptoCat offers end-to-end encryption for the Facebook Messenger users[9] too. Necessarily, secret chat applications must provide PFS (Perfect Forward Secrecy). PFS is provided in CryptoCat application with OTR. On the other side, Telegram does not provide the PFS[10].

CryptoCloak[11] is an application similar to the CryptoCat and Telegram in a way it provides secret chat. CryptoCloak uses a different approach - instead of sending encrypted content over the Internet, it sends sentences people use in everyday chat communication (so called "cheap chat"). Concerning the fact that any encrypted traffic might be store for further analysis by NSA traffic analysis engines[12], and cheap chat conversation is not point of interest, CryptoCloak will not be detected as suspicious.

4 CryptoCloak

CryptoCloak application was for the first time presented on BalkanCrypt Workshop[12]. The main idea was use of solid and secure cryptoalgorithms to provide secure chat communication, but do it in the clandestine way - instead of sending encrypted information,

mask them with cheap chat. Cheap chat - sentences such as: "Hello!", "How are you?", used in everyday chat communication, are the cloak for hiding encrypted information. Details about the way encrypted information are transformed into cheap chat sentences can be found in [11]. CryptoCloak is Java GUI (Graphical User Interface) chat application implemented using Java Swing API (Application Programming Interface). Implementation using Java programming language provides hardware independence, as well as operating system independence. During development period, since November 2013, until now, CryptoCloak changed two different APIs for chat communication (Figure 1).

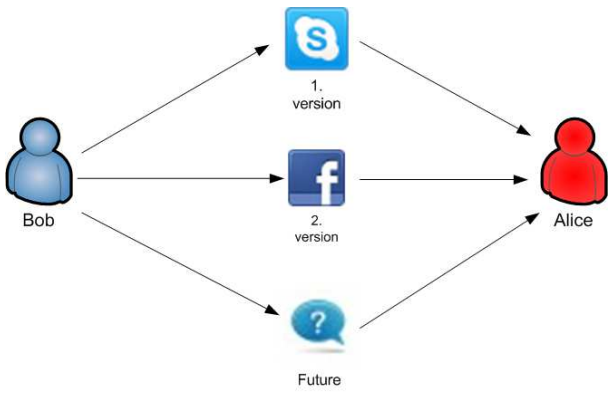

Figure 1: CryptoCloak versions.

First, Skype API for Java programming language was used. Unfortunately, this API was retired at the end of 2013, and CryptoCloak switched to Facebook Messenger API. Current research and implementation is based on this API. In the future, this might be changed, considering the fact that Facebook announced shutting-down the current Facebook Messenger API in 2015. Since Facebook Messenger API lies on XMPP, in future version "?" in Figure 1 can be replaced with any free available XMPP server. Second version of CryptoCloak is used at the moment for a proof of concept.

Similar to the chat applications described in Section 3, CryptoCloak provides end-to-end encryption for communication between its clients in order to keep personal data away from NSA's eyes and respect privacy. Sentences sent over Facebook Messenger server via CryptoCloak application might be stored there, but only on CryptoCloak client's side sentences will be conversed into the real information. Since CryptoCloak generates new key for every chat, it implements a form of PFS.

Major disadvantage in the current version of CryptoCloak is: to accomplish successful key exchange using cheap chat it takes around 30 minutes[11]. To an average end-user of instant chat messengers, this is probably unacceptable, and it has to be improved.

5 An improvement suggestion for the CryptoCloak

For accomplishing Diffie-Hellman key exchange process, Alice and Bob has to exchange two parameters: a and b. Parameters g (a primitive root modulo p) and prime p are public known, and they have been built into CryptoCloak application. Parameter a is calculated on Alice's side as: $g^x \ mod \ p$, where x is a random number. Similar, parameter b is calculated on Bob's side as: $g^y \ mod \ p$, where y is a random number.

To speed up the current key exchange process in CryptoCloak, parameters a and b, needed for Diffie-Hellman key exchange, can be sent as an e-mail message. It can be implemented the way is shown in Figure 2.

Using the same algorithm from the previous version[11], parameters will be converted into array of sentences, and, instead of sending these sentences via chat communication, they will be sent using legitimate e-mail account from well-known and appropriate e-mail server. Process of choosing well-known e-mail server has to be done very carefully. The main reason for this

lies in the fact that many of the companies which offer e-mail server access have an obligation to give the requested content of an e-mail message to the NSA.

When the particular parameter is received, it will be transformed into its real value, and the key will be calculated. The same process will be executed on both sides, Bob's and Alice's, and after successful Diffe-Hellman key exchange, they can start AES-CBC encrypted communication. User can send/receive e-mail message over/from different accounts. Splitting communication this way will be efficient and harder to follow. This technique will be similar to the the one the Tor[13] uses - based on twisty, hard to follow routes. Although, this provides exposure diversification - if communication is intercepted, it will still be hard to determine from where the message is sent or who is the sender.

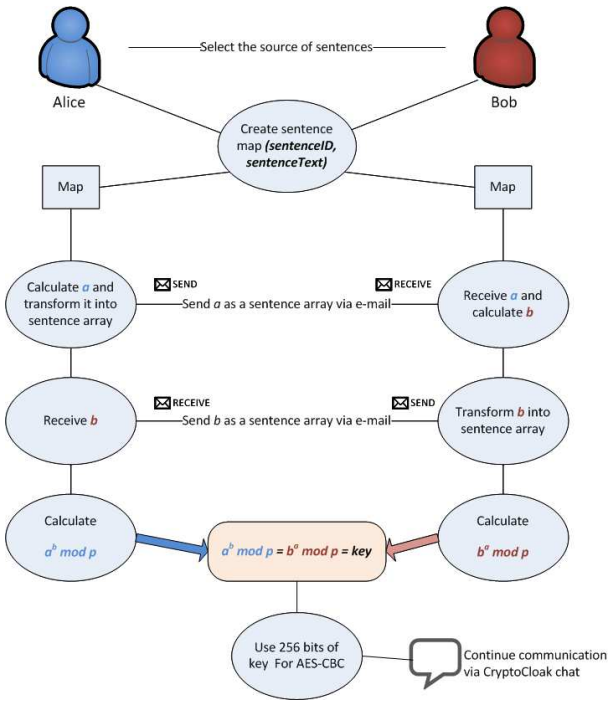

Figure 2: CryptoCloak improvement.

6 Further work

Suggested improvement is in an implementation phase. Since Java has an e-mail API, application development will continue in the same programming language as in previous versions. In the previous section, one improvement of the CryptoCloak application is presented under assumption that it can reduce overhead in the context of parameters exchange time. After implementation phase, experiments which prove melioration have to be done and comparative analysis using different e-mail servers has to be given. For security evaluation of the CryptoCloak application, threat model has to be defined and discussed, and the PFS still has to be proven. A way to cope with cryptanalysis techniques has to be given.

7 Conclusion

Privacy of individuals should not be threatened in any case. The CryptoCloak project has the aim protection against "surveillance/privacy" issues in the chat communication. To the best of author knowledge, Diffie-Hellman key exchange over the network, without sending uniform sequence of bytes, will not be detected by traffic analysis tools (spying engines). To accomplish successful key exchange with current version of CryptoCloak it takes around 30 minutes, which is too slow. In this paper an improvement for this issue is suggested. From theoretical aspect, this is a huge improvement in efficiency, but it has to be practical proven after implementation.

Acknowledgements

Dijana Vukovic, as a PhD student in the field of information security, is supported by the COINS Research School of Computer and Information Security.

References

[1] Edward Snowden and the NSA files timeline, Available online on http://www.theguardian.com/world/2013/jun/23/edward-snowden-nsa-files-timeline, last visited on 25.06.2014.

[2] Harding L.: The Snowden files - The Inside Story of the World's Most Wanted Man. The Guardian, 2014.

[3] Martin B.: Opposing Surveillance, IEEE Technology and Society Magazine, 29 (2), pp. 26-32, 2010.

[4] Schneier B., Privacy and Control, Available online on https://www.schneier.com/blog/archives/2010/04/privacy_and_con.html, last visited on 25.06.2014.

[5] EFF, International Principles on the Application of Human Rights to Communications Surveillance, Available online on https://en.necessaryandproportionate.org/text, last visited on 25.06.2014.

[6] Cryptocat, Available online on https://crypto.cat/, last visited on 25.06.2014.

[7] Telegram, Available online on https://telegram.org/, last visited on 25.06.2014.

[8] Telegram - Privacy Policy, Available online on https://telegram.org/privacy

[9] The Hacker News - Cryptocat offers End-to End Encryption For Facebook Messenger, Available online on http://thehackernews.com/2014/05/cryptocat-offers-end-to-end-encryption.html

[10] Telegram - FAQ for the Technically Inclined, Available online on https://core.telegram.org/techfaq#q-do-you-have-forward-secrecy, last visited on 25.06.2014.

[11] Vukovic, D., Gligoroski D., and Djuric Z.: On privacy protection in the Internet surveillance era. Proceedings of 11th International Conference on Security and Cryptography (SECRYPT), pp. 261-266, August 2014, Vienna, Austria.

[12] Vukovic, D.: The CryptoCloak Project. BalkanCrypt Kickoff Meeting and Workshop, Sofia, Bulgaria (2013)

[13] Tor project - About, Available online on https://www.torproject.org/about/overview.html.en, last visited on 25.06.2014.