NTNU – Trondheim
Norwegian University of
Science and Technology

Improvement proposal for the CryptoCloak application

Dijana Vukovic, Danilo Gligoroski and Zoran Djuric

{dijanav, danilog}@item.ntnu.no, zoran.djuric@etfbl.net

Outline

- Introduction
- What is the CryptoCloak?
- Improvement proposal
- Previous publications of the CryptoCloak application
- Further work

Introduction

- Snowden's revelation from 2013 -> privacy of the Internet communication has been disrupted.
- **Surveillance** can be defined as “close observation of a person or group, especially one under suspicion”.
- **Privacy** can simply be defined as “the right to be left alone”.
- **“Surveillance/privacy” issues** led to developing tools for anonymous communication over the Internet.
- Our approach to this issue - a prototype application called **CryptoCloak** application.

What is the CryptoCloak

- The basic idea of the CryptoCloak can be described as the following: use **solid** and **secure algorithms** that have been proved as secure, but do the encryption in a **clandestine** manner.

- **CryptoCloak** produces a fake real-time, dynamic cheap chat and into that chat it embeds the secret information.

- **Messages sent via CryptoCloak application are not encrypted**. Communication made this way is not point of interest for mass surveillance spying engines.

- **CryptoCloak's major disadvantage:** it takes around 30 minutes to accomplish successful Diffie-Hellman key exchange using cheap chat.

Improvement proposal

- For accomplishing Diffie-Hellman key exchange process, Alice and Bob have to exchange two parameters: *a* and *b*.
- Parameter a is calculated on Alice's side as: $g^x \bmod p$, where x is a random number. Similar, parameter b is calculated on Bob's side as: $g^y \bmod p$, where y is a random number.
- *a* and *b* can be sent as a part of an e-mail message. (Figure 1).

Improvement proposal (2)

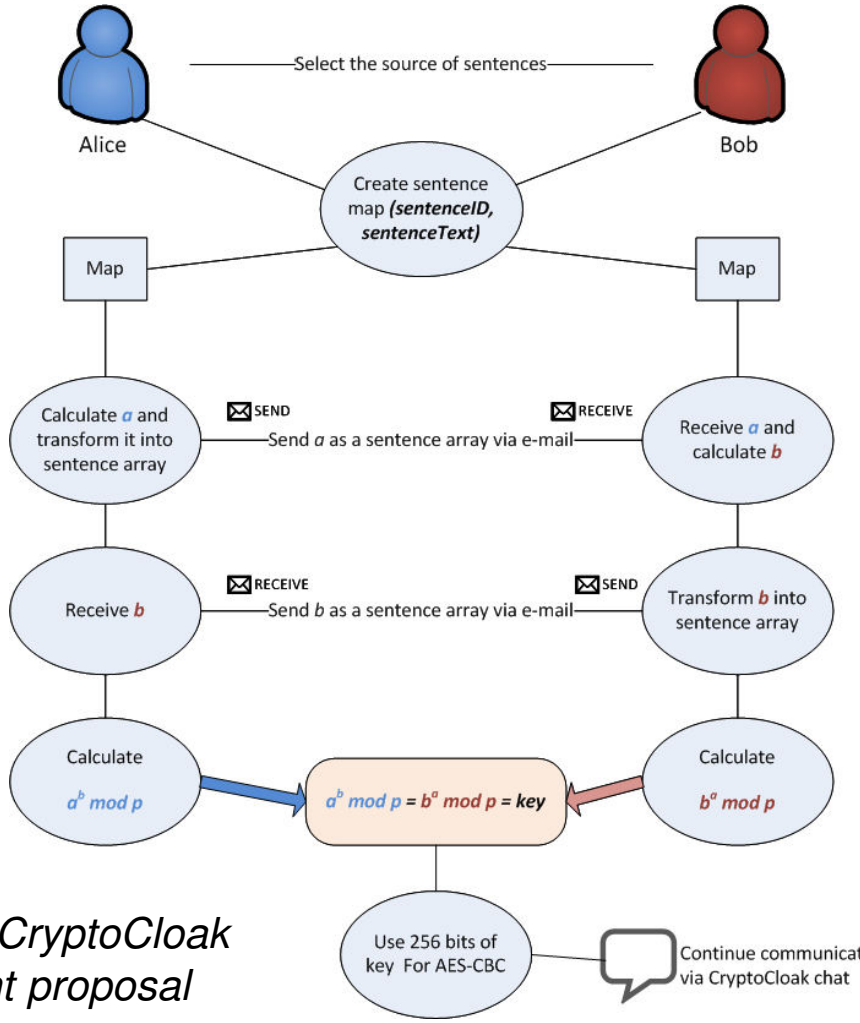

Figure 1. The CryptoCloak improvement proposal

NTNU – Trondheim
Norwegian University of Science and Technology

Improvement proposal (3)

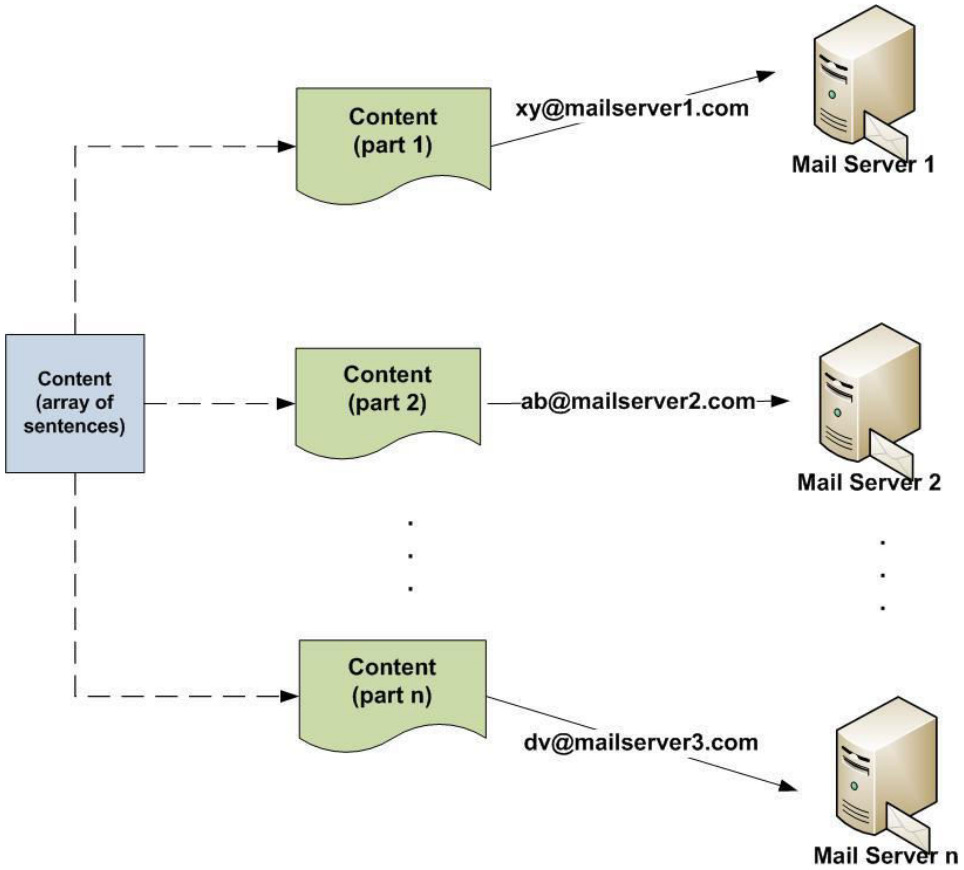

Figure 2. CryptoCloak – message sending over different accounts

- User can send/receive e-mail message over/from different accounts (Figure 2). Splitting communication this way will be efficient and harder to follow. This technique will be similar to the one the Tor 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.

NTNU – Trondheim
Norwegian University of
Science and Technology

Previous publications of the CryptoCloak application

- Vukovic, D., Djuric Z., and Gligoroski D.: ***CryptoCloak application - main idea, an overview and imrovement proposal***. (accepted for publishing on NISK 2014)

- 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.

Previous publications of the CryptoCloak application (2)

- Vukovic D.: ***CryptoCloak as a Protection Against Internet Surveillance***, Proceedings of INFOTEH 2014, pp. 909-912, March 2014, Jahorina, Bosnia and Herzegovina.

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

Further work

- Suggested improvement is in an implementation phase (using Java programming language). Proposed 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 to evaluate implemented improvement have to be done.
- 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.

NTNU – Trondheim
Norwegian University of
Science and Technology

Thank you for your attention!
Questions?