NTNU – Trondheim
Norwegian University of
Science and Technology

CryptoCloak – research overview

PhD student: Dijana Vukovic
Main supervisor: Danilo Gligoroski
Co-supervisor: Zoran Djuric

Outline

- Introduction
- CryptoCloak
- Related work
- Development phases and published papers
- Current phase of development (Openfire, Spark)
- Formal verification of the CryptoCloak protocol
- Open questions

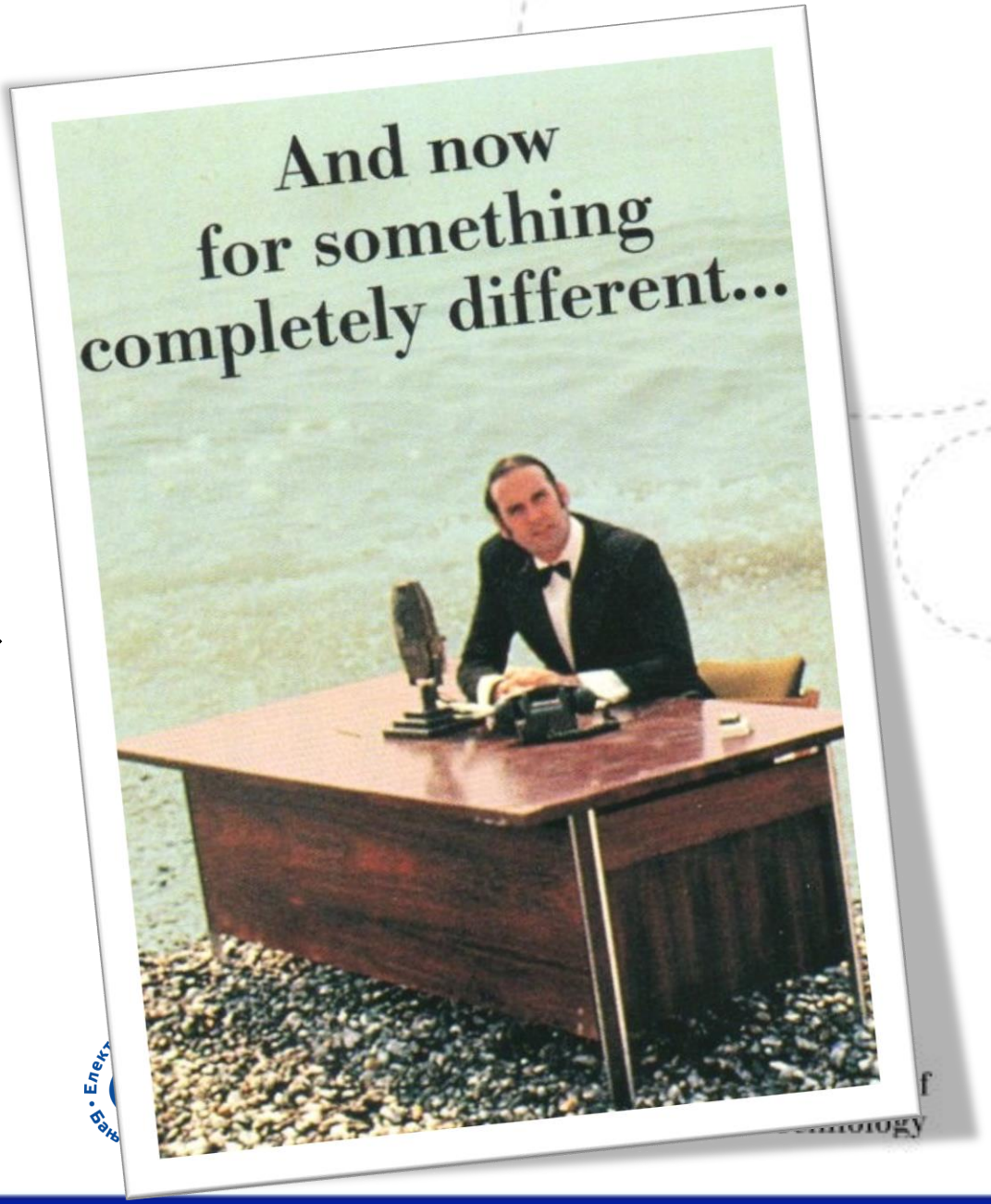
NTNU – Trondheim
Norwegian University of
Science and Technology

Introduction

- At first my research topic was focused on application of static source code analysis (SCA) for vulnerability detection.
- Static SCA of the Web-based applications written using Java programming language.
- Self-study course and research for the first semester were focused on the SCA and modelling of the hybrid static-dynamic analysis tool.
- D. Vuković, Z. Đurić, D. Gligoroski, **“Proposal for Expansion of STASEC Tool”**.

Introduction

- September 2013



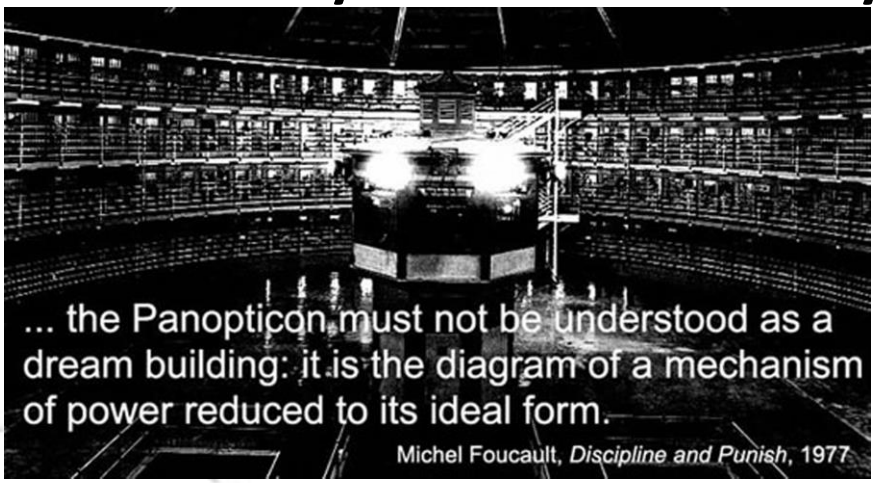
Introduction

- Snowden's revelation from July 2013 -> privacy of the Internet communication has been disrupted.
  - Abuse of Section 215 of the USA PATRIOT Act.
  - Lack of intellectual freedom.
  - Nine leading Internet companies.
- Luke Harding – “The Snowden Files: The Inside Story of the World's Most Wanted Man”.
- Glenn Greenwald – “No Place to Hide”.
- Documentary made by Laura Poitras – “CitizenFour”.

NTNU – Trondheim
Norwegian University of
Science and Technology

Introduction

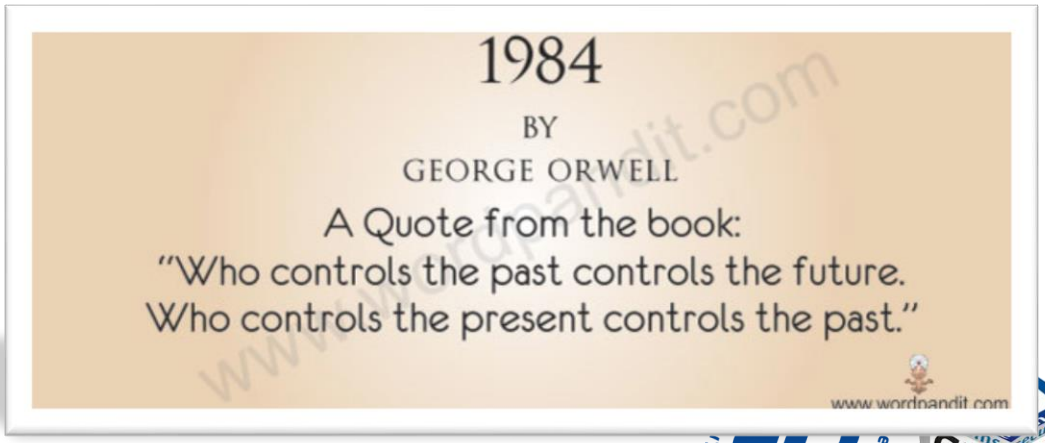
- Mass surveillance – something like *panopticon* (dated from 18th century).
- **"… And crucial to this design was that the inmates could not actually see into the panopticon, into the tower, and so they never knew if they were being watched or even when..."**



NTNU – Trondheim
Norwegian University of Science and Technology

Introduction

- Mass surveillance – George Orwell's *1984*.
- "There was, of course, no way of knowing whether you were being watched at any given moment."



NTNU – Trondheim
Norwegian University of
Science and Technology

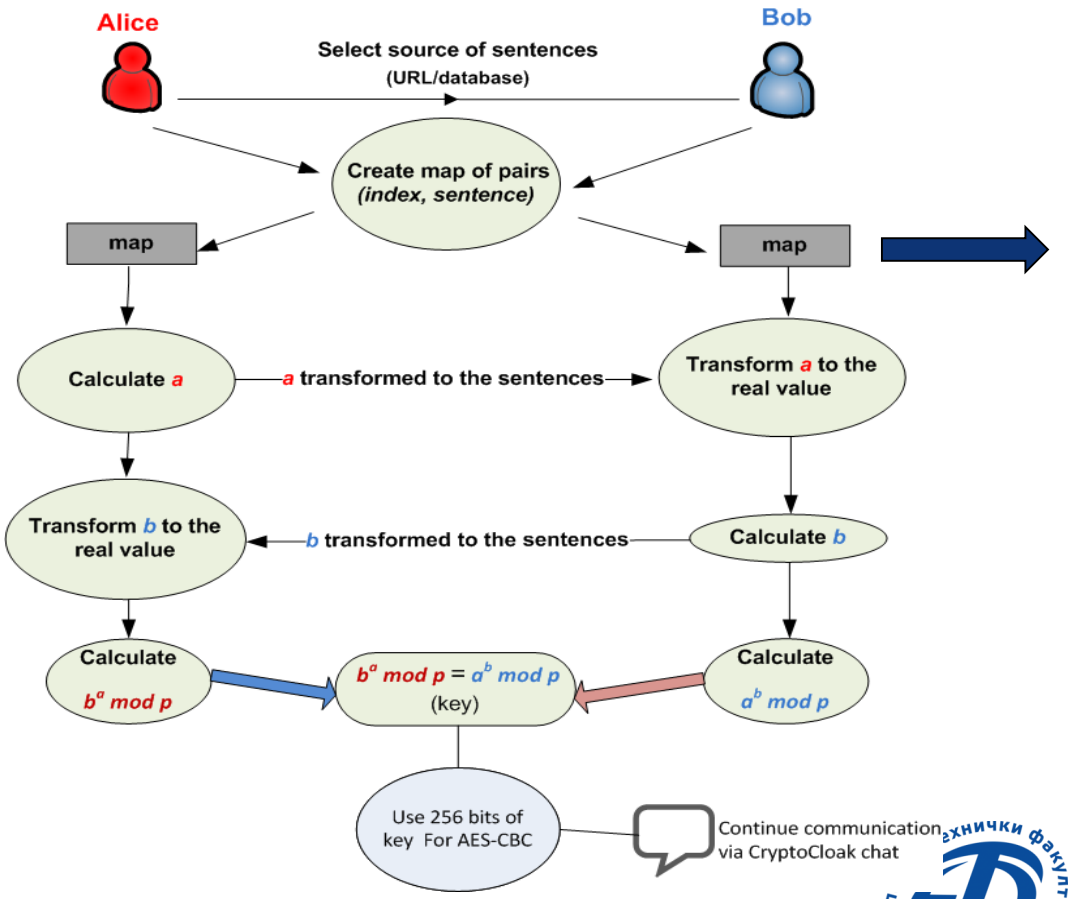
Introduction

- Last Week Tonight with John Oliver: Government surveillance (HBO)

CryptoCloak

- **The basic idea of the CryptoCloak** can be described as the following: use solid and secure algorithms, but do the encryption in a clandestine manner (Diffie-Hellman key-exchange).
- *CryptoCloak* produces a fake real-time, dynamic cheap chat and into that chat it embeds the secret information.
- **Chat messages sent via CryptoCloak application are not encrypted.** Communication made this way is not point of interest for mass surveillance spying engines.

CryptoCloak



Index	Sentence
0	Hi!
1	How are you?
2	Hello!
3	What kind of music do you like?
4	How old are you?

NTNU – Trondheim
Norwegian University of Science and Technology

CryptoCloak sentence mapping

- For accomplishing Diffie-Hellman key exchange process, Alice and Bob has to exchange two parameters: *a and b. Suppose that Alice and Bob agree to use p=47 and g=5. For the value of x Alice chooses 18, and for the value of y, Bob chooses 22. Both x* and *y are secret and random chosen value on Alice's and Bob's side, respectively.*
- On Bob's side, *b is calculated as 00011100. Suppose we have sn=5 and n=2.*
- It means that the binary value of b has to be split into 4 blocks with length 2, which gives us set {00, 01, 11, 00}, or integers {0, 1, 3, 0}. Obtained integers, used to gain indexes in sentences map in table, leads to the following set of sentences**: {"Hi!", "How are you?", "What kind of music do you like?", "Hi!"}**. This set will be sent over the network instead of the real value for b. Likewise, a will be conversed and sent.

NTNU – Trondheim
Norwegian University of
Science and Technology

CryptoCloak sentence mapping

- For accomplishing Diffie-Hellman key exchange process, Alice

The larger sentences set is, the block size will be bigger, and the number of sentences representing one parameter will be smaller – key-exchange will be accomplished faster.

Sentences set was only around 4000 sentences long at the time.

To exchange one parameter, over 150 sentences had to be exchanged – almost 30 minutes…

This set will be sent over the network instead of the real value for b. Likewise, a will be conversed and sent.

NTNU – Trondheim
Norwegian University of
Science and Technology

Related work

- **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, and OTR is used to provide conversation privacy.

- **Telegram** messenger is a cross-platform whose clients are open source, providing to an average end-user: privacy protection, accessibility to messages from different devices, and secure communication without any limits in the size of chat messages (MTProto protocol).

- https://www.eff.org/secure-messaging-scorecard

NTNU – Trondheim
Norwegian University of
Science and Technology

Related work

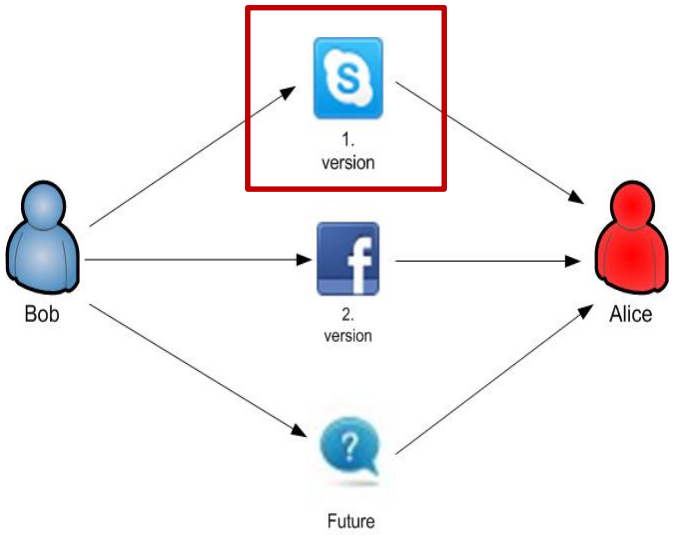
- *"CryptoCloak does not use the steganography. It does not embed the information in some other existing information. It produces a fake real-time, dynamic cheap chat and there it embeds the secret information."*

- After some conferences and discussions with people from this area of research, we came to the conclusion that CryptoCloak might be using one special type of steganography - steganography by cover synthesis.

Related work

- In steganography by cover synthesis, Alice creates the stego Work without recourse to a cover Work.
- An interesting real-world example of such a system has been described at the end of “Between Silk and Cyanide”, by Leo Marks. The code, called “Windswept,” which was used by British spies in World War II, works in the following manner.
- Big book of conversations with alternate wordings for each line, and even alternate courses that the conversation could take. Each line was associated, arbitrarily, with a number. By selecting different phrases from the book, British spies could thus encode sequences of numbers in perfectly innocuous conversations.

Development phases and published papers

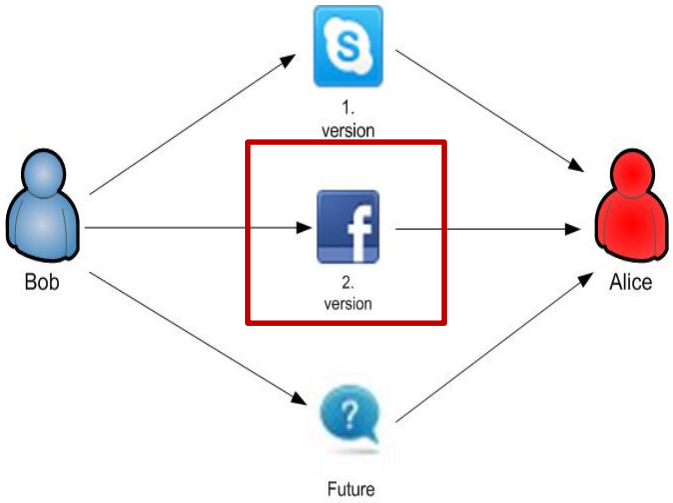


Skype API – retired in December 2013.

Published paper:

D. Vuković, "*CryptoCloak as a Protection Against Internet Surveillance*", Conference INFOTEH 2014, Jahorina, Bosnia and Herzegovina, 2014;

Development phases and published papers



Facebook API – retired in March 2015.

Published paper:

D. Vuković, Z. Đurić, "On Privacy Protection in the Internet Surveillance Era", SECRYPT 2014, pp. 261 - 266, Aug, 2014

Development phases and published papers – Facebook API

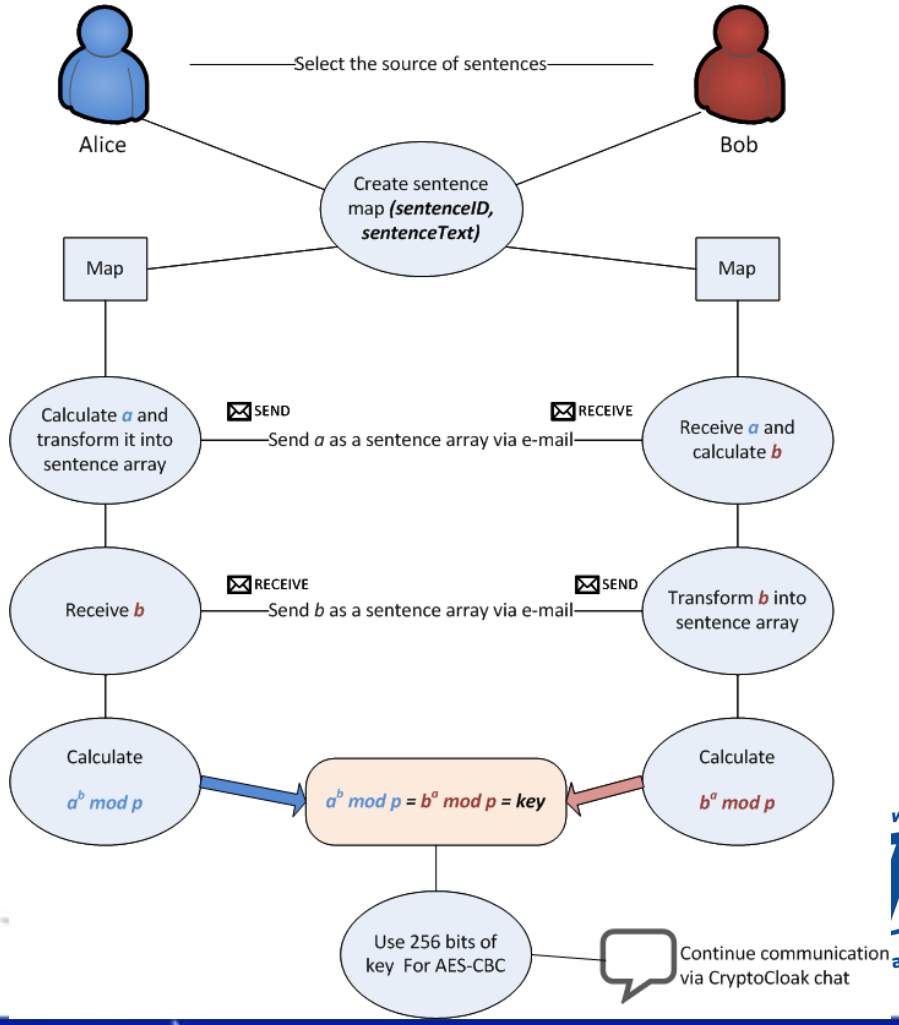
- The source of sentences was expended with conversation sentences from two TV shows: “Friends” and “How I met your mother?” on **size of around 50000 relatively short sentences**.
- Using these sentences, we made some statistic overview for continued conversation using CryptoCloak protocol after successful key-exchange to determine who might be potential users of our application.

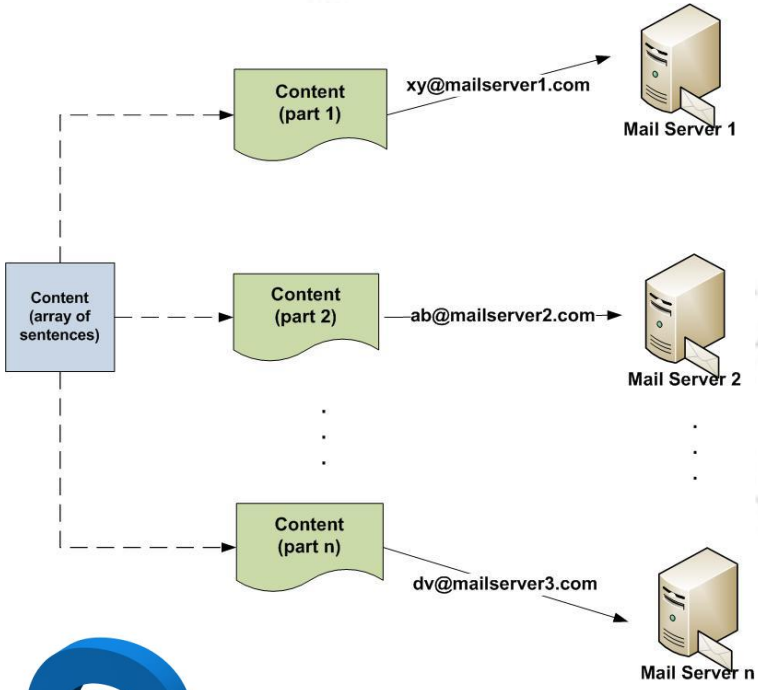
Development phases and published papers – Facebook API

- Analysis:

Sentence	Mapped into	Time for exchange (s)
Hello there!	24	105
Are you free to go out tonight?	34	95
I'm going bowling, sorry, maybe next weekend…	58	279
The CryptoCloak project uses cryptographic algorithms for key exchange and encryption that have been selected by the cryptographic community as solid and secure algorithms BUT it is doing the encryption in a clandestine manner.	184	917

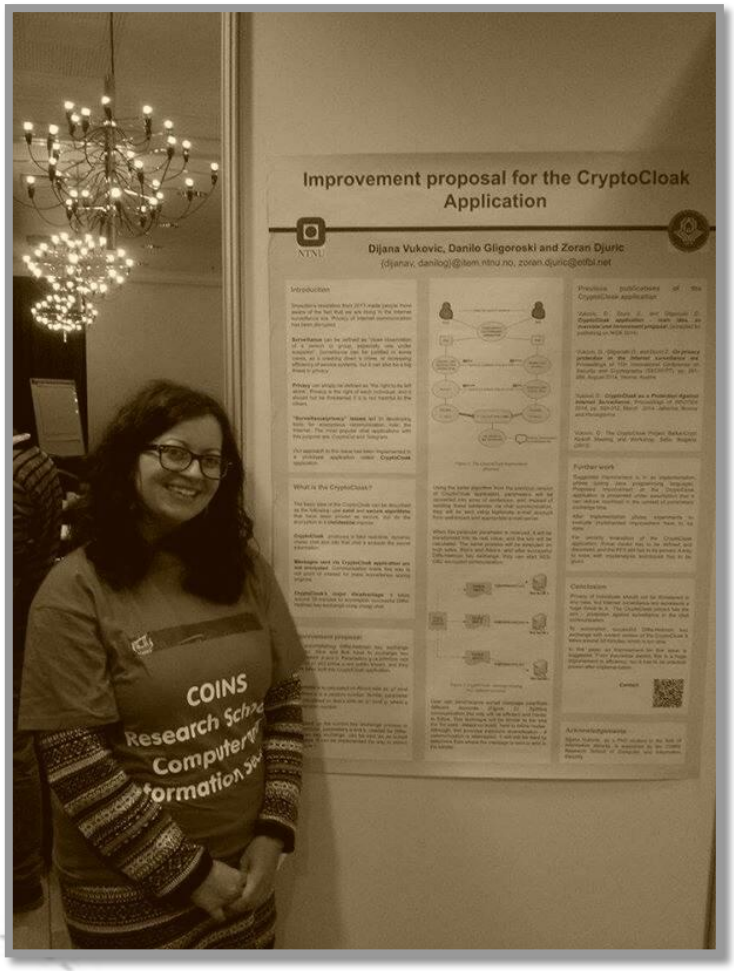
Development phases and published papers – e-mail version





NTNU – Trondheim
Norwegian University of Science and Technology

Development phases and published papers – e-mail version

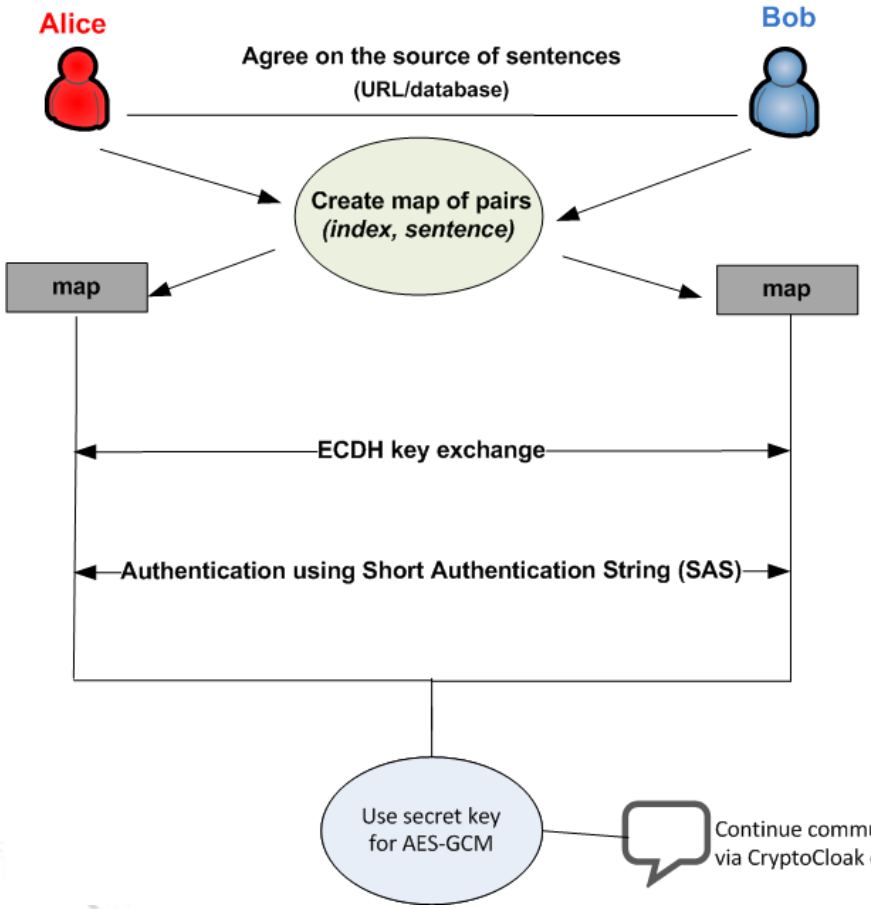


- Poster **“Improvement proposal for the CryptoCloak Application”** was presented on NordSec 2014.
- Vukovic, D., Djuric Z., and Gligoroski D.: “**CryptoCloak application - main idea, an overview and improvement proposal”** (NISK 2014).
- D. Vuković, Z. Đurić, D. Gligoroski, **“CryptoCloak - improvement proposal implementation”**, Proceedings of 22nd Telecommunications forum TELFOR 2014, Belgrade, Serbia.

Електротехнички факултет • Бања Лука • 1962 •

NTNU – Trondheim
Norwegian University of Science and Technology

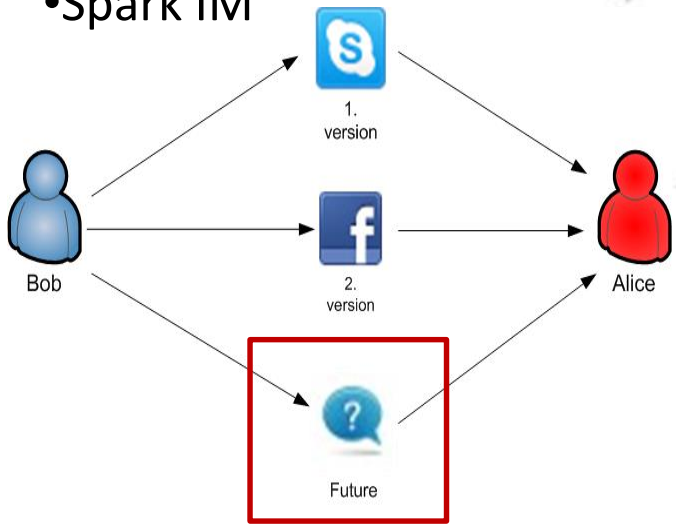
Development phases and published papers



? – what will we use next?

Our infrastructure:

- Openfire XMPP server
- Spark IM



NTNU – Trondheim
Norwegian University of Science and Technology

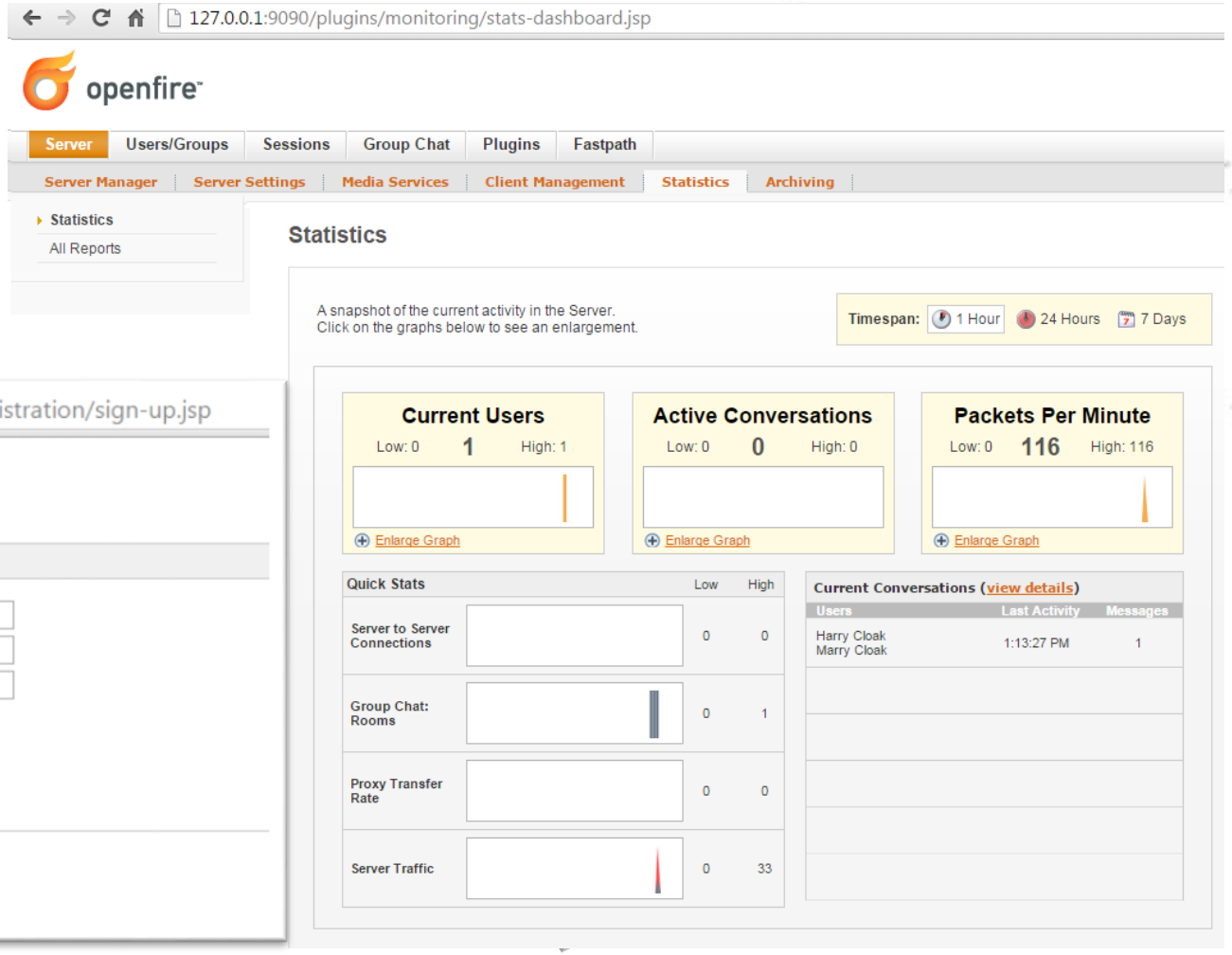
Current phase of development (Openfire, Spark)

- **Openfire** is a real time collaboration (RTC) server licensed under the Open Source Apache License. It uses the only widely adopted open protocol for instant messaging, XMPP (also called Jabber). Openfire is incredibly easy to setup and administer, but offers rock-solid security and performance.

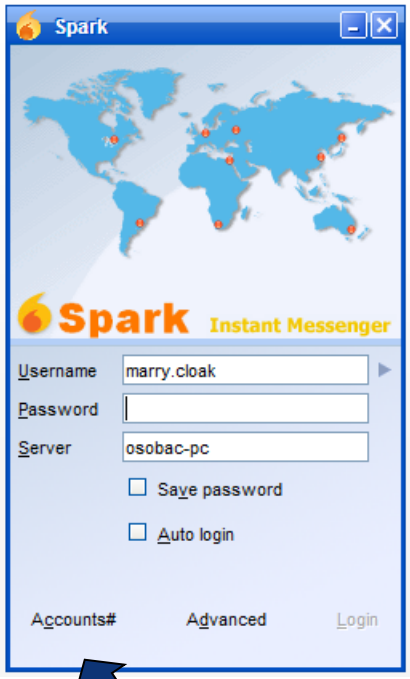
- **Spark** is an Open Source, cross-platform IM client optimized for businesses and organizations. It features built-in support for group chat, telephony integration, and strong security. It also offers a great end-user experience with features like in-line spell checking, group chat room bookmarks, and tabbed conversations.

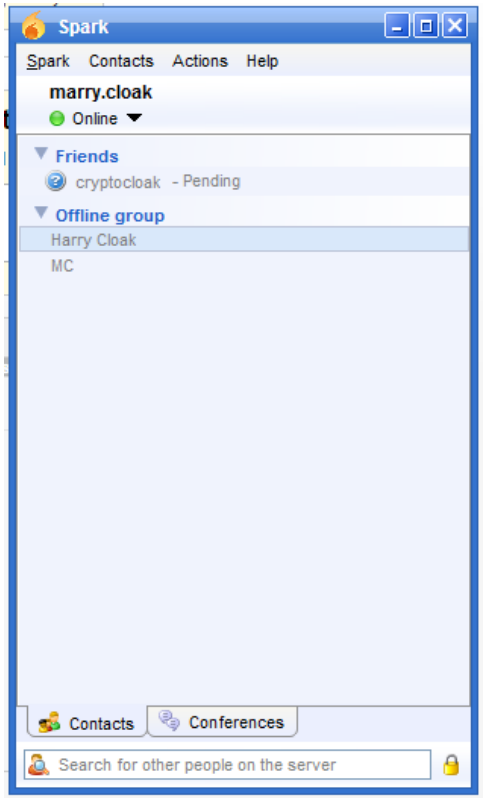
NTNU – Trondheim
Norwegian University of Science and Technology

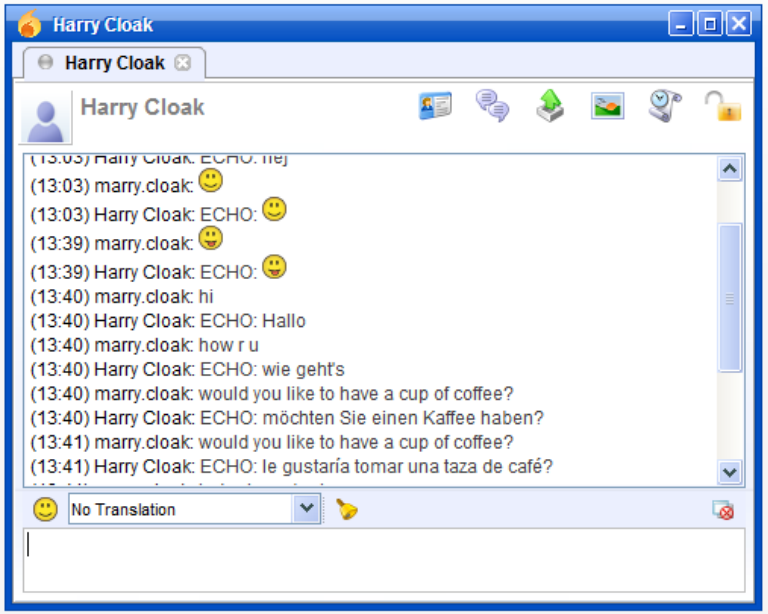
Current phase of development (Openfire, Spark)



Current phase of development (Openfire, Spark)





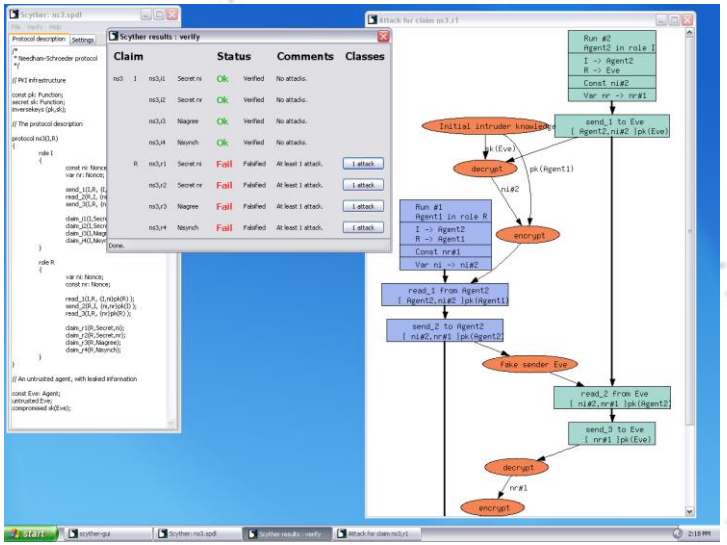


Users can also register through the Spark

NTNU – Trondheim
Norwegian University of Science and Technology

Current phase of development (Openfire, Spark)

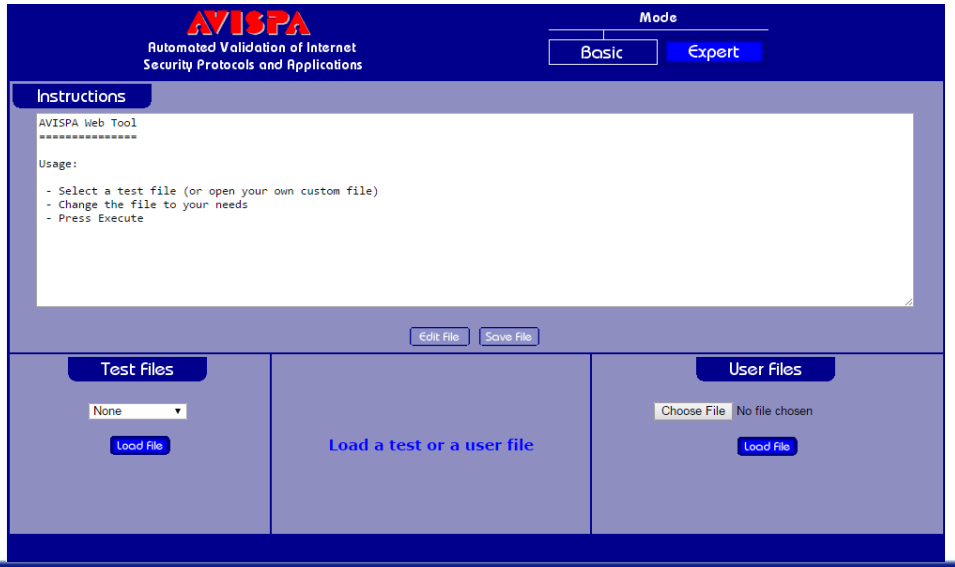
Formal verification of the CryptoCloak protocol



- Writing formal protocol specification.
- Analyze it using AVISPA and/or Skyther tool.
- Make fixes if it is necessary.

- Outcome:

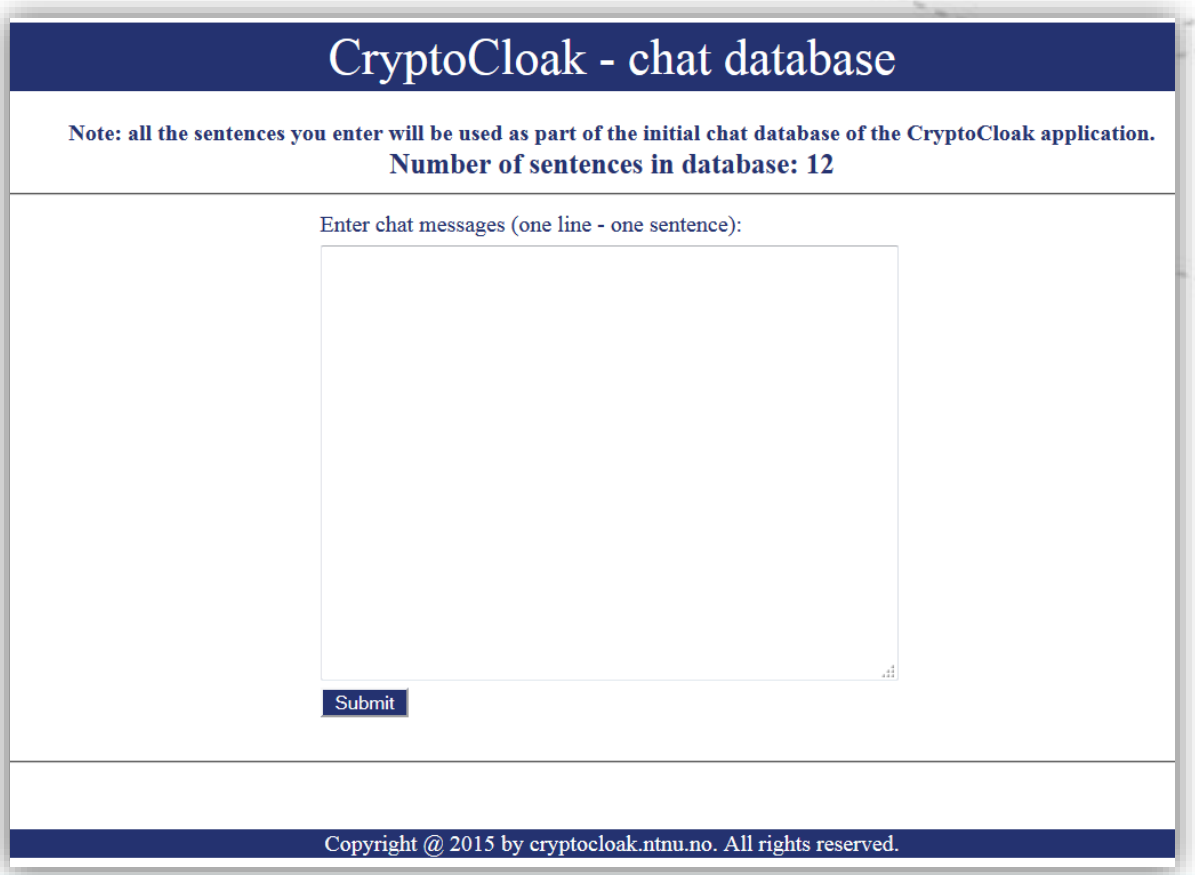
  publishing of the results.



Open questions

- Source of sentences expansion with the real chat messages: http://cryptocloak.item.ntnu.no:8080/cryptocloakchatsource/

- Spark plug-in testing
- Changing sending algorithm
- “Real world” testing
- Formal verification



Thanks for the attention!

Вјеровали или не,
у Норвешкој се Зимске школе одржавају и у мају. „Забавник" ми је овај пут правио друштво у планинском мјесту Финсе, чија жељезничка станица се налази на 1222 m надморске висине. Финсе је иначе познат и по томе што се овдје снимао филм „Ратови звијезда V: Империја узвраћа ударац". Лијеп поздрав са још хладног и снјежног Сјевера!
ДИЈАНА ВУКОВИЋ

"If we knew what we were doing, it wouldn't be called research, would it?"

Електротехнички факултет • Бања Лука • 1962

NTNU – Trondheim
Norwegian University of Science and Technology