Conversation Security using KleeQ

Part II Project

Pavel Berkovich

University of Cambridge

Supervised by Dr. Richard Clayton

February 4, 2016

UNIVERSITY OF CAMBRIDGE

Outline

UNIVERSITY OF CAMBRIDGE

Problems of P2P secure communication

Problem 1: Contact Discovery

How do we know where to send our messages?

Problem 2: Trust Establishment

How do we know our peers are who they say they are?

Problem 3: Conversation Security

How do we encrypt the messages, what data do we attach to them, and what security protocols do we perform?

Problem 4: Transport Privacy

What is the mechanics for actually sending the message so as to hide the message metadata (sender, recepient, time, size etc)?

CAMBRIDGE

Problems of P2P secure communication

Problem 1: Contact Discovery

How do we know where to send our messages?

Problem 2: Trust Establishment

How do we know our peers are who they say they are?

Problem 3: Conversation Security

How do we encrypt the messages, what data do we attach to them, and what security protocols do we perform?

Problem 4: Transport Privacy

What is the mechanics for actually sending the message so as to hide the message metadata (sender, recepient, time, size etc)?

CAMBRIDGE

KleeQ (Readon et al, 2006)

- conversation security protocol for P2P *ad-hoc* group communication
- security properties:
  - confidentiality of message content
  - message integrity
  - forward and backward secrecy
  - message authorship repudiation
  - conversation participation repudiation
  - anonymity preserving
- very hacky and unstable implementation in Python

UNIVERSITY OF CAMBRIDGE

Goals of the project

Brief reminder

Goal 1: Implementation

Implement the protocol in Java. See how it performs, test scalability limits.

Goal 2: Messenger Prototype

Build a simple prototype of a messenger to show that the protocol works.

UNIVERSITY OF CAMBRIDGE

Accomplishments

Architecture

- Asynchronous communicaiton with callbacks
- Inheritance hierarchy of message types

Some protocol components

- Group establishment
- Derivation of common secret + encryption/decryption

Interface

A simple CLI interface, for testing.

Secondary Components

- Online contact discovery ("address book")
- Store-n-forward service

To-Do's

Patching Algorithm

An somewhat unusual algorithm for message exchange suggested by paper. Currently done by pseudo-multicast.

Transcript Verification

Procedure for verifying the global transcript, specified in the paper. No integrity check at the moment.

Improved key mangement

Independent recomputation of common secret based on the results of transcript verification. Gives forward/backward secrecy.

UNIVERSITY OF CAMBRIDGE

Challenges Encountered

Challenge 1: Protocol gaps

The original paper omits *a lot* of detail. Have to re-design some parts independently.

Challenge 2: Phase order problem

To test a conversation security protocol, have to write a lot of "scaffolding" first. This needs to be done *before*, not after writing the protocol.

Challenge 3: Private IP addresses

P2P is made complicated by most hosts not having public IP addresses. Had to write a simple store-and-forward service.

UNIVERSITY OF CAMBRIDGE

Challenges Encountered

Challenge 1: Protocol gaps

The original paper omits *a lot* of detail. Have to re-design some parts independently.

Challenge 2: Phase order problem

To test a conversation security protocol, have to write a lot of "scaffolding" first. This needs to be done *before*, not after writing the protocol.

Challenge 3: Private IP addresses

P2P is made complicated by most hosts not having public IP addresses. Had to write a simple store-and-forward service.

UNIVERSITY OF CAMBRIDGE

Challenges Encountered

Challenge 1: Protocol gaps

The original paper omits *a lot* of detail. Have to re-design some parts independently.

Challenge 2: Phase order problem

To test a conversation security protocol, have to write a lot of "scaffolding" first. This needs to be done *before*, not after writing the protocol.

Challenge 3: Private IP addresses

P2P is made complicated by most hosts not having public IP addresses. Had to write a simple store-and-forward service.

UNIVERSITY OF CAMBRIDGE

Challenges Encountered

Challenge 1: Protocol gaps

The original paper omits *a lot* of detail. Have to re-design some parts independently.

Challenge 2: Phase order problem

To test a conversation security protocol, have to write a lot of "scaffolding" first. This needs to be done *before*, not after writing the protocol.

Challenge 3: Private IP addresses

P2P is made complicated by most hosts not having public IP addresses. Had to write a simple store-and-forward service.

UNIVERSITY OF CAMBRIDGE

Timing

Date	Milestone
14-02-2016	Patching Algorithm implemented
21-02-2016	Transcript integrity verification done
28-02-2016	Key rotation implemented
06-03-2016	Clean up and bundle into a usable library
21-04-2016	Dissertation written up

UNIVERSITY OF CAMBRIDGE

Q&A

Do you have any questions?

UNIVERSITY OF CAMBRIDGE

Thank you!

UNIVERSITY OF CAMBRIDGE