FH AACHEN
UNIVERSITY OF APPLIED SCIENCES

Fachhochschule Aachen

Campus Jülich

Fachbereich: Medizintechnik und Technomathematik

Studiengang: Technomathematik

Secure Multi-Party Computation for Decentralized Distributed Systems

Masterarbeit von Frederic Klein

Diese Arbeit wurde betreut von:

1. Prüfer: Prof. Dr. rer. nat. Alexander Voß
2. Prüfer: Dr. Stephan Jonas

Aachen, Dezember, 2016

Diese Arbeit ist von mir selbständig angefertigt und verfasst. Es sind keine anderen als die angegebenen Quellen und Hilfsmittel benutzt worden.

Frederic Klein ....
Unterschrift

Abstract

In recent years gamification has become a part of many areas of our daily routine. In regard to our personal life, companies like Amazon or Runtastic can base their gamification approach on publicly sharing personal achievements and statistics to improve user commitment. In contrast, gamification concerning our work life has to satisfy much higher privacy demands. Since comparison is a key component for the gamification approach, privacy protecting computations of system wide statistical values (for example minimum and maximum) are needed. The solution comes in the form of secure multi-party computation (SMPC), a subfield of cryptography. Existing frameworks for SMPC utilize the Internet Protocol, though access to the Internet or even a local area network (LAN) cannot be provided in all environments. Facilities with sensible measuring systems, e.g. medical devices in hospitals, often avoid Wi-Fi to reduce the risk of electromagnetic interference. To be able to utilize SMPC in environments with Wi-Fi restrictions, this thesis studies the characteristics of mobile ad hoc network (MANET)s and proposes the design of a SMPC framework for MANETs, especially based on Bluetooth technology, and the implementation as a C library.

Since MANETs have a high probability for network partition, a centralized architecture for the computation and data preservation is unfavorable. Therefor a distributed database based on the blockchain is implemented in the framework. Typical problems of distributed systems are addressed with the implementation of algorithms for clock synchronization and coordinator election as well as protocols for the detection of computation partners and data distribution are provided. Since the framework aims to provide distributed computations of statics for comparison, protocols for secure addition and a secure comparison are implemented, enabling the computation of minimum, maximum and average.

Devices of diverse computational power will be used to verify the applicability for wearables and Internet of Things (IoT) grade devices. Also field-tests with a smart phone ad hoc network (SPAN)(20-50 nodes) will be conducted to evaluated real life use cases. In contrast, the security of the framework and attack scenarios will be discussed.

In summary this thesis proposes a framework for SMPC for decentralized, distributed systems.

Contents

List of Figures

List of Tables

List of Acronyms

IoT Internet of Things.

LAN local area network.

MANET mobile ad hoc network.

SMPC secure multi-party computation.

SPAN smart phone ad hoc network.

Chapter 1

Introduction

5-10%, including motivation, general audience

In the last couple of years gamification has found it's way into many areas of our daily life. In regard to our personal life, companies like Amazon or Runtastic can base their gamification approach on publicly sharing personal achievements and statistics to improve user commitment. In contrast, gamification concerning our work life can have much higher privacy demands. Since comparison is a key component for the gamification approach, privacy protecting computations of system wide statistical values (for example minimum and maximum) are needed. The solution comes in the form of SMPC, a subfield of cryptography.

Existing frameworks for SMPC utilize the Internet protocol, though access to the Internet or even a LAN cannot be provided in all environments. Especially many hospitals tend to avoid Wi-Fi to reduce the risk of electromagnetic interference with medical devices.

To be able to utilize SMPC in environments with Wi-Fi restrictions, this thesis studies the characteristics of mesh-networks and proposes describes the design of a SMPC framework for mesh-networks.

Context

Restatement of the problem

Restatement of the response

Roadmap

Chapter 2

Background

10-15%; thorough review of the state of the art; informed audience

2.1 Case Study: "The Hygiene Games"

Gamification

Wireless Networks in Hospitals

2.2 Secure Multi-Party Computation

Secure Addition Protocol

Secure Comparison Protocol

Differential Privacy

Existing Frameworks

2.3 Mobile Ad Hoc Networks

- continuously self-configuring
- self-forming
- self-healing
- infrastructure-less
- peer-to-peer

- Difference to mesh: mobility of nodes

Smart Phone Ad Hoc Network

Example: firechat

Comparison to Wi-Fi Direct

- SPAN support multi-hop relays
- Wi-Fi Direct since Android 4.0
- Wi-Fi Direct: Soft AP

Wi-Fi Based SPAN

Bluetooth Based SPAN

2.4 Distributed Computing

Coordinator Election

Chapter 3

Design

15-20%; explains complete processing chain; explains what methods are used; for someone that wants to know what was done in detail

Chapter 4

Implementation

15-20%; details on the implementation; for someone who wants to continue the work

Chapter 5

Evaluation

5-15%; outcome; how was it tested; for supervisor

Chapter 6

Discussion

5-15%; outcome for a design-reader

Chapter 7

Conclusion

5-10%; outcome for a introduction-reader

Appendix A

Some name

Nulla malesuada porttitor diam. Donec felis erat, congue non, volutpat at, tincidunt tristique, libero. Vivamus viverra fermentum felis. Donec nonummy pellentesque ante. Phasellus adipiscing semper elit. Proin fermentum massa ac quam. Sed diam turpis, molestie vitae, placerat a, molestie nec, leo. Maecenas lacinia. Nam ipsum ligula, eleifend at, accumsan nec, suscipit a, ipsum. Morbi blandit ligula feugiat magna. Nunc eleifend consequat lorem. Sed lacinia nulla vitae enim. Pellentesque tincidunt purus vel magna. Integer non enim. Praesent euismod nunc eu purus. Donec bibendum quam in tellus. Nullam cursus pulvinar lectus. Donec et mi. Nam vulputate metus eu enim. Vestibulum pellentesque felis eu massa.