# Proposal with Schedule

Yiwen Tang Jiayi Zhang Yawei Zhang Rui Zhang

February 26, 2020

## 1 Scope and Importance

We mainly focus on implementing an additional protection mechanism above the Transport Layer Security (TLS) protocol to ensure the users to retrieve secure data from the network transfers. For getting data from web servers, this can be done in two ways, from the server side and the client side. The server side would require the modification of the TLS protocol and a third party auditor can be used in the client side to attest a TLS connection. Our work will focus on the network between the server and the client, some detailed descriptions of TLS and HTTP and utilize some properties of the cryptography algorithms to achieve our desired results. In this project, we will implement the algorithms, deploy the server and the client side to generate verification between different servers, and finally find ways to improve the performance of the algorithms. Furthermore, we also want to find more application scenarios for the additional protection mechanism. For example, how to deploy them on top of IoT data infrastructure, which requires credible real-world data acquired from the sensors.

Although TLS protocol is already used to encrypt network data for other network protocols such as HTTP protocol, there still exists attacks aiming at SSL/TLS such as man-in-the-middle attack. The attacker would establish separate connections with the server and client, disguise as a legal connection endpoint, and intercept normal network data to alter or insert illegal data without being recognized. Users are currently unable to prove to a third party the content they have observed on a particular website. One of the most popular methods for users to document and share content they watch on the Internet are screenshots that are trivial to falsify, which is inefficient and inconvenient. However, TLSNotary allows a client to provide evidence to a third-party auditor that certain web traffic occurred between himself and a server. The evidence is irrefutable as long as the auditor trusts the server's public key. In this way, the client can know whether the data has been intercepted or altered. Apart from web scenarios, TLSNotary can also be applied to the blockchain, physical sensors and so on to provide reliable real data. Through this research, we would learn how TLS protocol works to ensure data security, how the properties of RSA, hash function and hash digest can be applied to optimize TLS protocol and the experience of deploying the web servers and the clients.

## 2 Related Work

Oracle was originally designed to solve how to provide real external information to the blockchain, because the blockchain cannot actively capture data from the outside world. Oracle is like a bridge linking the blockchain to the real world, providing a way to load external information without trust. There are some examples of this undeniable mechanism: IoT sensors providing real-world data, distributed blockchain oracles, an implementation based on a trusted computing environment, and implementation based on TLS/SSL protocol modification.

In the field of the Internet of Things, sensors mainly work in the sensing layer, solving the data acquisition problems between the real world and the network world. But not all data can be obtained from sensors, such as the results of sports competitions, the price of stock securities. Distributed systems can deliver trusted real-world data. For example, Augur is the first distributed application of Ethereum, but prediction markets creating a heavy reliance on human input and severely constraining their scope and data types. Implementation based on a trusted computing environment can provide a credible external trigger condition for smart contracts. As the name implies, it relies on the third-party computing environment. TLSNotary is just based on the TLS/SSL protocol, splitting the client into two parts - auditee and auditor. TLSNotary provides a service that allows a third-party auditor to attest to a web connection between the server and the client.

Actually, according to current research, Oracle not only can be used in the Blockchain area, but it can also be applied in various areas of life. TLSNotary is closer to the internet area. Using TLSNotary could solve many internet scenarios that users want to provide data from a web page as evidence. For example, people routinely provide printouts as evidence of a transaction, or provide proof of funds to support a visa application, or just provide data from a web URL. TLSNotary as an Internet-wide undeniable mechanism that allows user data to be retrieved from web pages in a provably secure manner. That is, the data is definitely the same as the server by using TLSNotary.

## 3 Schedule

- Week 1 - Week 2 (Feb.17th - March 1st)

  Milestone: Compare TLSNotary and TLS regarding security and efficiency. Research related algorithms and technology, such as asymmetric crypto, homomorphic encryption, pseudorandom function.

  - Analyze the paper of TLSNotary
  - Mid-semester progress report (Due March 3rd)

- Week 3 - Week 4 (March. 2nd - March 15th)

  Milestone: Implement function module of Auditee which acts as a communication end in Python; conduct a unit test.

  - Deploy production environment
  - Implement Auditee algorithm
  - Test case samples and result documents for the Auditee communication function unit

- Week 4 - Week 5 (March. 16th - March 29th)

  Milestone: Complete function module of Auditor authentication and conduct unit tests; integrate two modules together.

  - Implement Auditor algorithm
  - Test case samples and result documents for the Auditor authentication function unit
  - Integration test and analysis for two modules

- Week 6 - Week 7 (March. 30th - April 12th)

  Milestone: Deploy on the cloud.

  - Production environment setup
  - Analysis document on function indicator, performance indicator and security indicator

- Week 8 - Week 9: (April. 13 - April. 26)

  Milestone: test and improve on the issues of the current TLSNotary version; develop a web page with TLSNotary.

  - Operation manual document of web page
  - A project poster for the poster session (Due April 27th)
  - Final report (Due Friday, May 1st)

## 4 Deliverables

- Mid-semester progress report
- Implement auditee & auditor algorithm
- Test results on communication and authentication function units
- Deploy project environment
- Result analysis on function indicator, performance indicator and security indicator
- Develop a web page with TLSNotary
- Operation manual document of web page
- A project poster
- Final report