Master’s Thesis: Risk Mitigation of using SSL/TLS-certificates as a Binding between Smart Contract-based Systems and the Web

Jan Felix Hoops, 16.11.2020, Kick-off Presentation

Chair of Software Engineering for Business Information Systems (sebis)
Faculty of Informatics
Technische Universität München
wwwmatthes.in.tum.de

Outline

1. Background
2. Motivation
3. Problem Statement
4. Research Questions
5. Approach
6. Timeline

Background

Lack of Smart Contract Owner Authentication
There is no widely adopted, standardized way of authenticating the owner of an Ethereum Smart Contract. This is a security risk.

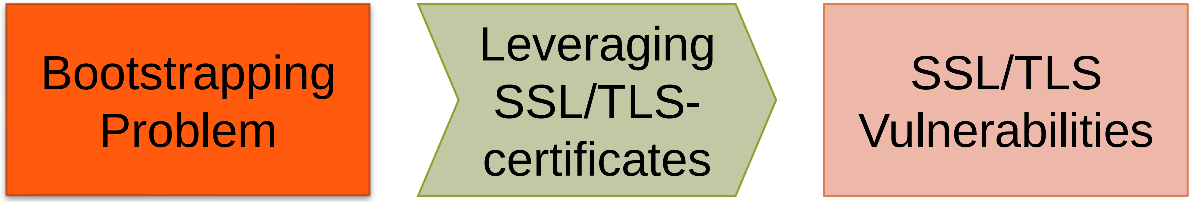
One important reason for this deficit is the **bootstrapping problem**.

TLS endorsed Smart Contracts (TeSC)
This proposal by Gallersdörfer envisions an authentication infrastructure leveraging SSL/TLS-certificates of the web.

Motivation

TeSC is a compelling solution to the problem of authenticating Smart Contracts.

TeSC‘s arguably biggest strength comes at a price.



Bootstrapping Problem

Leveraging SSL/TLS-certificates

SSL/TLS Vulnerabilities

Problem Statement (1/2)

Unintended use-case for X.509
Risks of using certificates for Smart Contract authentication are very different.

Differences between TeSC verifier types
Supporting on-chain and off-chain verifiers means that all new mechanisms have to be designed and evaluated for both.

Level of control over certificate issuance
With influence over the certificate store (i.e. on-chain), it might be possible to prevent certificate mis-issuance.

Problem Statement (2/2)

Deterministic on-chain verification
Changes to on-chain verification must ensure that different nodes executing still arrive at the same conclusion.

Usability
Security and usability are commonly conflicting goals and we do not want to deter users from using TeSC.

Cost
Any security mechanisms added must not compromise the economic viability of TeSC.

Research Questions (1/2)

RQ1 What are actively used security mechanisms for the SSL/TLS-PKI on the web?

a) What requirements were set by their creators?

RQ2 What attack vectors (ab-)using the SSL/TLS-PKI exist for TeSC?

RQ3 How can TeSC be augmented to mitigate the risk of using SSL/TLS-certificates?

a) Can mechanisms from RQ1 be adapted to TeSC and the Blockchain?
b) How effective are the newly added security mechanisms?
c) How costly are the newly added security mechanisms?

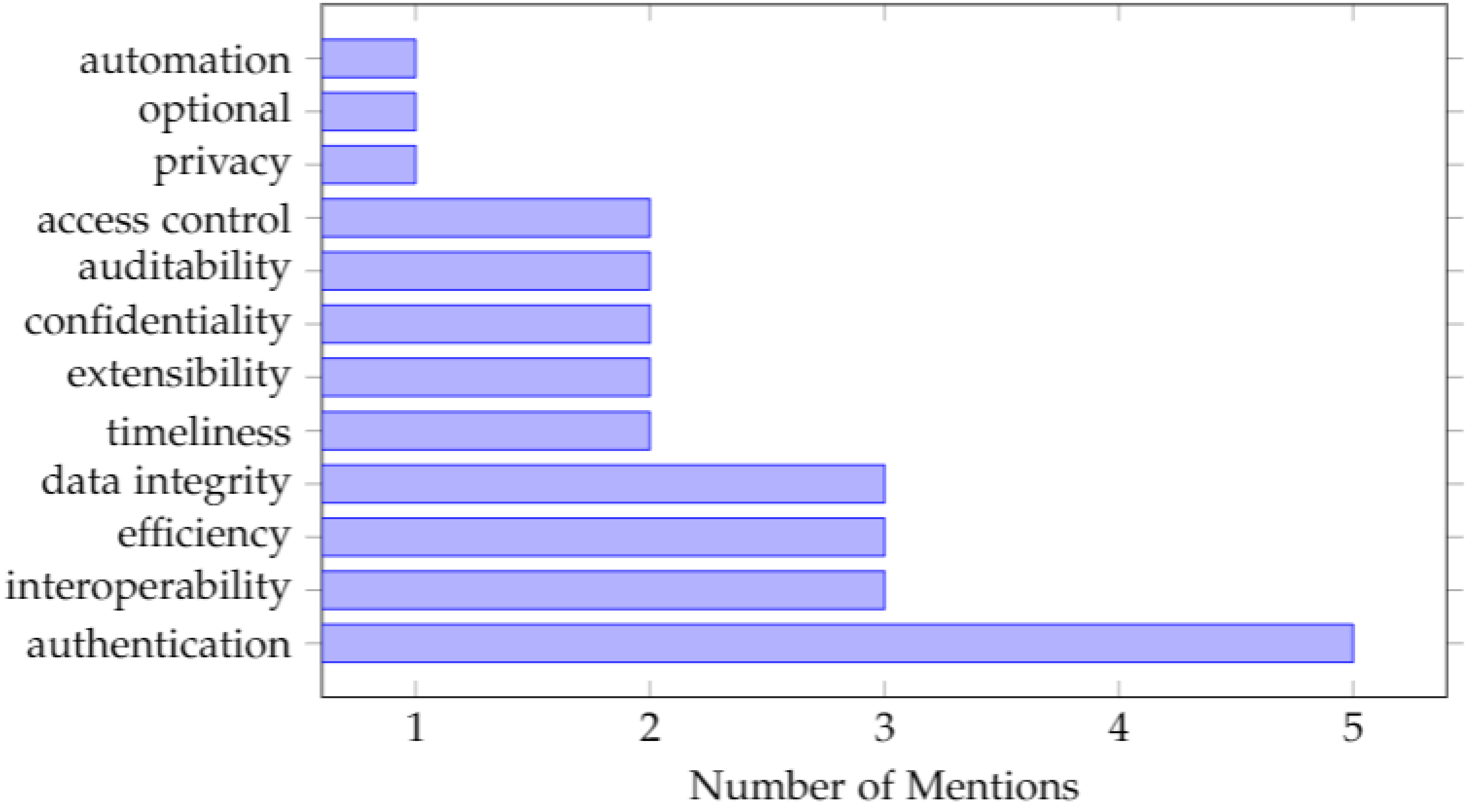
Research Questions (2/2)

RQ1 What are actively used security mechanisms for the SSL/TLS-PKI on the web?

a) What requirements were set by their creators?

Systems of interest:

- TLS
- IPsec
- DNSSEC
- CT
- CRL
- OCSP
- CRLite



Approach

1 Literature Research

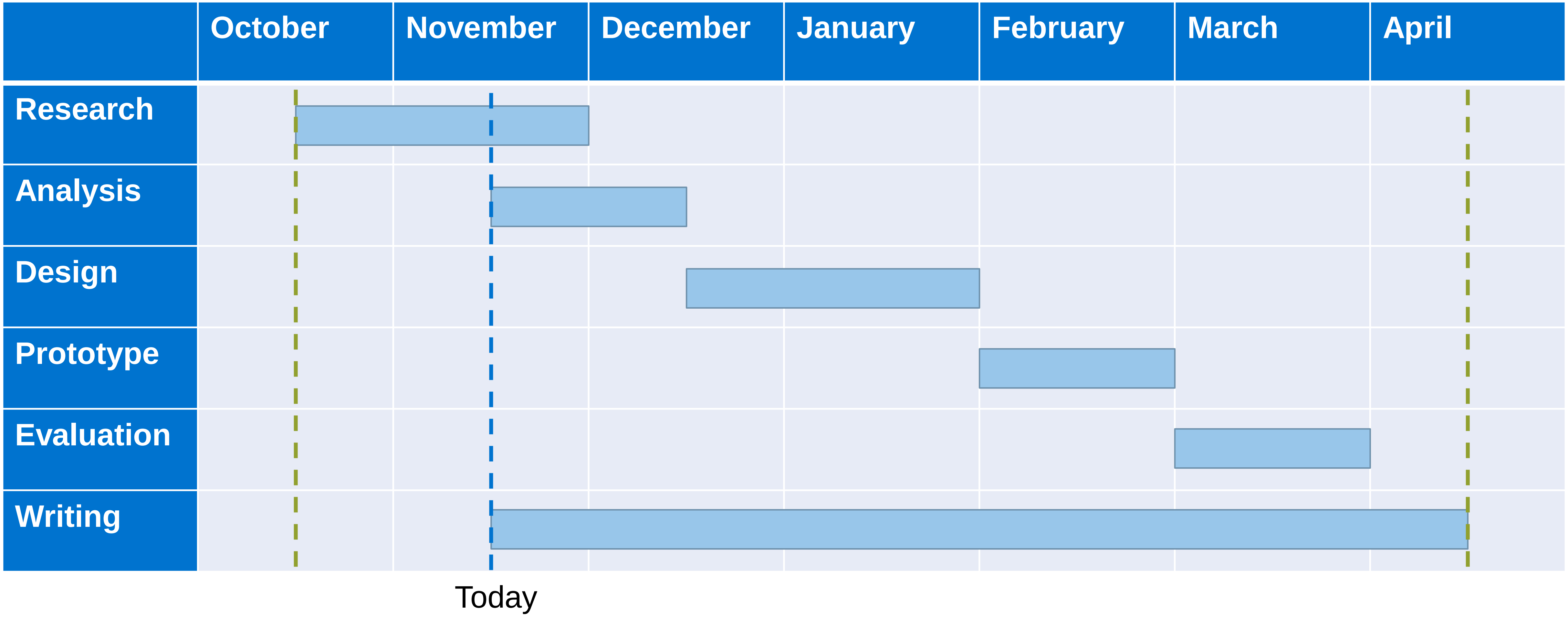
2 TeSC Vulnerability Analysis

3 Security Mechanism Design

4 Prototype Implementation

5 Evaluation

Timeline



October

November

December

January

February

March

April

Research

Analysis

Design

Prototype

Evaluation

Writing

Today

B. Sc.

Jan Felix Hoops
felix.hoops@tum.de

Technische Universität München
Faculty of Informatics
Chair of Software Engineering for Business
Information Systems

Boltzmannstraße 3
85748 Garching bei München

Tel +49.89.289.
Fax +49.89.289.17136